A Framework for the Construction of Golay Sequences

Frank Fiedler, Jonathan Jedwab, and Matthew G. Parker

***Abstract*—In 1999 Davis and Jedwab gave an explicit algebraic normal form for $m! \cdot 2^{h(m+2)}$ ordered Golay pairs of length 2^m over $\mathbb{Z}_{2^h}$, involving $m!/2 \cdot 2^{h(m+1)}$ Golay sequences. In 2005 Li and Chu unexpectedly found an additional 1024 length 16 quaternary Golay sequences. Fiedler and Jedwab showed in 2006 that these new Golay sequences exist because of a "cross-over" of the aperiodic autocorrelation function of certain quaternary length 8 sequences belonging to Golay pairs, and that they spawn further new quaternary Golay sequences and pairs of length 2^m for $m > 4$ under Budišin's 1990 iterative construction.**

The total number of Golay sequences and pairs spawned in this way is counted, and their algebraic normal form is given explicitly. A framework of constructions is derived in which Turyn's 1974 product construction, together with several variations, plays a key role. All previously known Golay sequences and pairs of length 2^m over $\mathbb{Z}_{2^h}$ can be obtained directly in explicit algebraic normal form from this framework. Furthermore, additional quaternary Golay sequences and pairs of length 2^m are produced that cannot be obtained from any other known construction. The framework generalizes readily to lengths that are not a power of 2, and to alphabets other than $\mathbb{Z}_{2^h}$.

***Index Terms*—autocorrelation function, algebraic normal form, complementary, construction, cross-over, Golay sequence, quaternary, shared autocorrelation property.**

I. INTRODUCTION

Let H be an even positive integer. A *sequence of length n over $\mathbb{Z}_H$* is a sequence of values $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$, where each $a_i \in \mathbb{Z}_H$. Let ξ be a primitive H-th root of unity and define the *aperiodic autocorrelation function* of $\boldsymbol{a}$ to be

$$C_{\boldsymbol{a}}(u) := \sum_{i=0}^{n-1-u} \xi^{a_i - a_{i+u}} \text{ for integer } u \text{ satisfying } 0 \le u < n.$$

A pair $(\boldsymbol{a}, \boldsymbol{b})$ of sequences of length n over $\mathbb{Z}_H$ is called a *Golay complementary pair* (often abbreviated to *Golay pair*) of length n over $\mathbb{Z}_H$ if

$$C_{\boldsymbol{a}}(u) + C_{\boldsymbol{b}}(u) = 0 \quad \text{for all integer } u \text{ satisfying } 0 < u < n.$$

A sequence $\boldsymbol{a}$ is called a *Golay sequence* if it forms a Golay pair with some sequence $\boldsymbol{b}$. The name is in honor of Golay [7], who introduced this condition for the case $H = 2$ in 1949.

This paper is concerned with Golay sequences of length 2^m over $\mathbb{Z}_H$. Mostly we are interested in the case $H = 2^h$ for integer $h \ge 1$, and especially in the *binary* case $H = 2$ and the *quaternary* case $H = 4$. In 1999 Davis and Jedwab [4] gave an explicit algebraic normal form for $m! \cdot 2^{h(m+2)}$ ordered Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ of length 2^m over $\mathbb{Z}_{2^h}$, involving $m!/2 \cdot 2^{h(m+1)}$ Golay sequences. These pairs are obtained by taking $H = 2^h$ in (1) (see Section II). We will call Golay pairs and sequences of the form (1) *standard*.

It was believed for several years that there are no non-standard Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$, but in 2005 Li and Chu [11] unexpectedly found 1024 length 16 non-standard quaternary Golay sequences by computer search. Li and Kao [12] showed that these new sequences arise from concatenation or interleaving of quaternary length 8 Golay pairs. In 2006 Fiedler and Jedwab [5] gave a full explanation of the structure of the new sequences by showing that their existence depends on a "shared autocorrelation property" of certain standard quaternary length 8 Golay sequences. This property had previously been observed in [4] but its significance had been overlooked. (In hindsight the papers [10] and [3], which use computer search to determine the number of non-standard quaternary ordered Golay pairs of length 8 and 16 as 512 and 8192 respectively, also contain clues as to the existence of the new length 16 Golay sequences; see [5] for further discussion.) Currently the only known examples of Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$ having the shared autocorrelation property are those described in [5].

Golay's foundational paper [8] shows how to construct a binary Golay pair of length $2n$ by interleaving or concatenating the sequence elements of a binary Golay pair of length n. The paper [8] also constructs a binary Golay sequence of length 2^m directly using a generalized Boolean sum construction. Budišin [2] showed that this generalized Boolean sum construction can be realized by iterated interleaving and concatenation of an initial trivial binary Golay pair of length 1, provided that "gaps" (meaning zero elements) are allowed in the constructed sequence at intermediate steps. Budišin's construction [2] also applies to non-binary Golay pairs of length 2^m, in particular Golay pairs over $\mathbb{Z}_{2^h}$. Paterson [14] showed that the standard Golay sequences having $H = 2^h$, that were presented explicitly in [4] as an extension of Golay's generalized Boolean sum construction, can be obtained iteratively using Budišin's construction.

It is then natural to ask: what quaternary Golay sequences and pairs are obtained when Budišin's iterative construction is applied to the 512 non-standard length 8 quaternary ordered Golay pairs? We know from [5] that the Golay sequences and pairs of length 16, 32, 64, ... spawned in this way are non-standard, and that the number of Golay sequences and pairs of length 16 spawned is 1024 and 8192 respectively (matching

F. Fiedler is with Department of Mathematics, Wesley College, 120 North State Street, Dover, DE 19901, USA. Email: FiedleFr@wesley.edu. He is grateful to Simon Fraser University for hospitality during 2004–2005.

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6. Email: jed@sfu.ca. He is supported by NSERC of Canada.

M.G. Parker is with Department of Informatics, High Technology Center in Bergen, University of Bergen, Bergen 5020, Norway. Email: Matthew.Parker@ii.uib.no. He is grateful to Simon Fraser University for hospitality during 2006.

the counts in [11] and [3] obtained by exhaustive search). But [5] could not determine the number of quaternary Golay sequences and pairs of length 2^m spawned for $m > 4$, even when the iterative construction is restricted to just interleaving and concatenation (not allowing gaps in intermediate steps).

The principal objective of this paper is to determine the number of quaternary Golay sequences and pairs of length 2^m ($m \geq 4$) obtained by applying Budišin's iterative construction to the 512 non-standard length 8 quaternary ordered Golay pairs, and moreover to find the algebraic normal form of the constructed sequences and pairs explicitly. Although the algebraic normal forms appear rather complex when written out, they completely describe the constructed sequences.

A second objective of the paper is to identify, from the many known explicit and iterative constructions, a framework from which all known Golay sequences and pairs of length 2^m over $\mathbb{Z}_{2^h}$ can be obtained in explicit algebraic normal form. The explicit constructions include Golay's generalized Boolean sum construction [8, (13)] and its extension to generalized Boolean functions by Davis and Jedwab [4]. The iterative constructions include: Golay's concatenation and interleaving of a binary Golay pair [8, (9), (10)]; Golay's block-interleaving of two binary Golay pairs [8, (11), (12)]; Budišin's iterative construction using permutations and roots of unity [2]; and Turyn's product construction for producing a binary Golay pair from two shorter binary Golay pairs [16, Lemma 5]. We shall see that, once the standard Golay pairs (1) are given, the key construction among all of these is Turyn's, together with several variations that we shall derive. These variations allow us to construct directly and explicitly the Golay sequences and pairs of length 2^m over $\mathbb{Z}_{2^h}$ that would be obtained by applying Budišin's construction iteratively.

A third objective of this paper is to demonstrate that the framework described is powerful enough to produce further Golay sequences and pairs of length 2^m over $\mathbb{Z}_{2^h}$ that cannot be obtained by applying Budišin's construction iteratively to a non-standard length 8 quaternary Golay pair.

The rest of the paper is organized in the following way. Section II introduces further notation and definitions, particularly for algebraic normal form and the shared autocorrelation property. Section III reviews Turyn's construction in some detail, because of its importance in our constructive framework. Section IV develops variations on Turyn's construction, in which Golay pairs are used to control the iterative interleaving and concatenation of other Golay pairs. Section V uses the constructive framework to determine which Golay sequences and pairs are spawned by an initial ordered Golay pair $(\boldsymbol{a}, \boldsymbol{b})$ of length 2^r, and applies this result to the 512 non-standard quaternary ordered Golay pairs of length 8. Section VI summarizes the results of the paper, clarifies the relationship to other work, and lists some open questions.

Figure 1 is a Venn diagram illustrating the intersections of the constructions described in this paper. For each lemma in the diagram, the annotations describe restrictions on its use. Figure 2 is a flowchart showing how the constructed sets of quaternary Golay sequences are obtained. Table I gives counts of the number of standard and non-standard quaternary Golay sequences and quaternary ordered Golay pairs of length 2^m. All currently known quaternary Golay sequences and pairs included in these counts can be obtained via the flowchart shown in Figure 2.

II. Notation and definitions

In this section we introduce some notation and definitions, particularly for algebraic normal form and the shared autocorrelation property. Throughout, H will be an even positive integer and ξ will be a primitive H-th root of unity.

As before, a sequence of length n over $\mathbb{Z}_H$ is a sequence of values $\boldsymbol{a} = (a_0, a_1, \dots, a_{n-1})$, where each $a_i \in \mathbb{Z}_H$. In phase shift keying with H phases, the sequence elements a_i represent data to be communicated, and the sequence $\boldsymbol{a}$ corresponds to the *complex modulated sequence* $(\xi^{a_0}, \xi^{a_1}, \dots, \xi^{a_{n-1}})$ of roots of unity. The *generating function associated with* $\boldsymbol{a}$ is the polynomial

$$A(x) := \sum_{i=0}^{n-1} \xi^{a_i} x^i.$$

Straightforward manipulation shows that

$$A(x)\overline{A(x^{-1})} = n + \sum_{u=1}^{n-1} C_{\boldsymbol{a}}(u)x^{-u} + \sum_{u=1}^{n-1} \overline{C_{\boldsymbol{a}}(u)}x^u,$$

where bar represents complex conjugation. It follows that if $\boldsymbol{a}, \boldsymbol{b}$ form a Golay pair of length n and $A(x)$, $B(x)$ are the associated generating functions then

$$A(x)\overline{A(x^{-1})} + B(x)\overline{B(x^{-1})} = 2n.$$

In this case we call $(A(x), B(x))$ a *complementary function pair*. (The converse, that the sequences associated with a complementary function pair form a Golay pair, is true provided that we work with complex modulated sequences $\boldsymbol{a}, \boldsymbol{b}$ of arbitrary complex numbers, and use the complex modulated definitions $C_{\boldsymbol{a}}(u) := \sum_{i=0}^{n-1-u} a_i \overline{a_{i+u}}$ and $A(x) := \sum_{i=0}^{n-1} a_i x^i$ for the aperiodic autocorrelation function and generating function respectively. Such sequences do not in general correspond to phase shift keying, and some of their elements may even be 0. Although our primary interest in this paper is Golay pairs over $\mathbb{Z}_H$, the constructions in Section IV can be generalized to these Golay pairs of arbitrary complex numbers.)

A sequence $\boldsymbol{a} = (a_0, \dots, a_{2^m-1})$ of length 2^m over $\mathbb{Z}_H$ can be described by means of its algebraic normal form. A *generalized Boolean function* is a function $f : \mathbb{Z}_2^m \to \mathbb{Z}_H$. Let $0 \leq i < 2^m$ and let $(i_1, \dots, i_m)$ be the binary expansion of i, where i_1 is the most significant bit. Let $f_j(x_1, \dots, x_m) = x_j$ be the indicator function for i_j (which is bit j in the binary representation of i). The indicator functions $f_1, \dots f_m$ give rise to 2^m monomials

$$\begin{aligned}
&1,\\
&x_1, x_2, \dots, x_m,\\
&x_1x_2, x_1x_3, \dots, x_{m-1}x_m,\\
&\vdots\\
&x_1x_2\cdots x_m.
\end{aligned}$$

Multiplication of indicator functions corresponds to the logical AND operation, and addition corresponds to logical XOR.

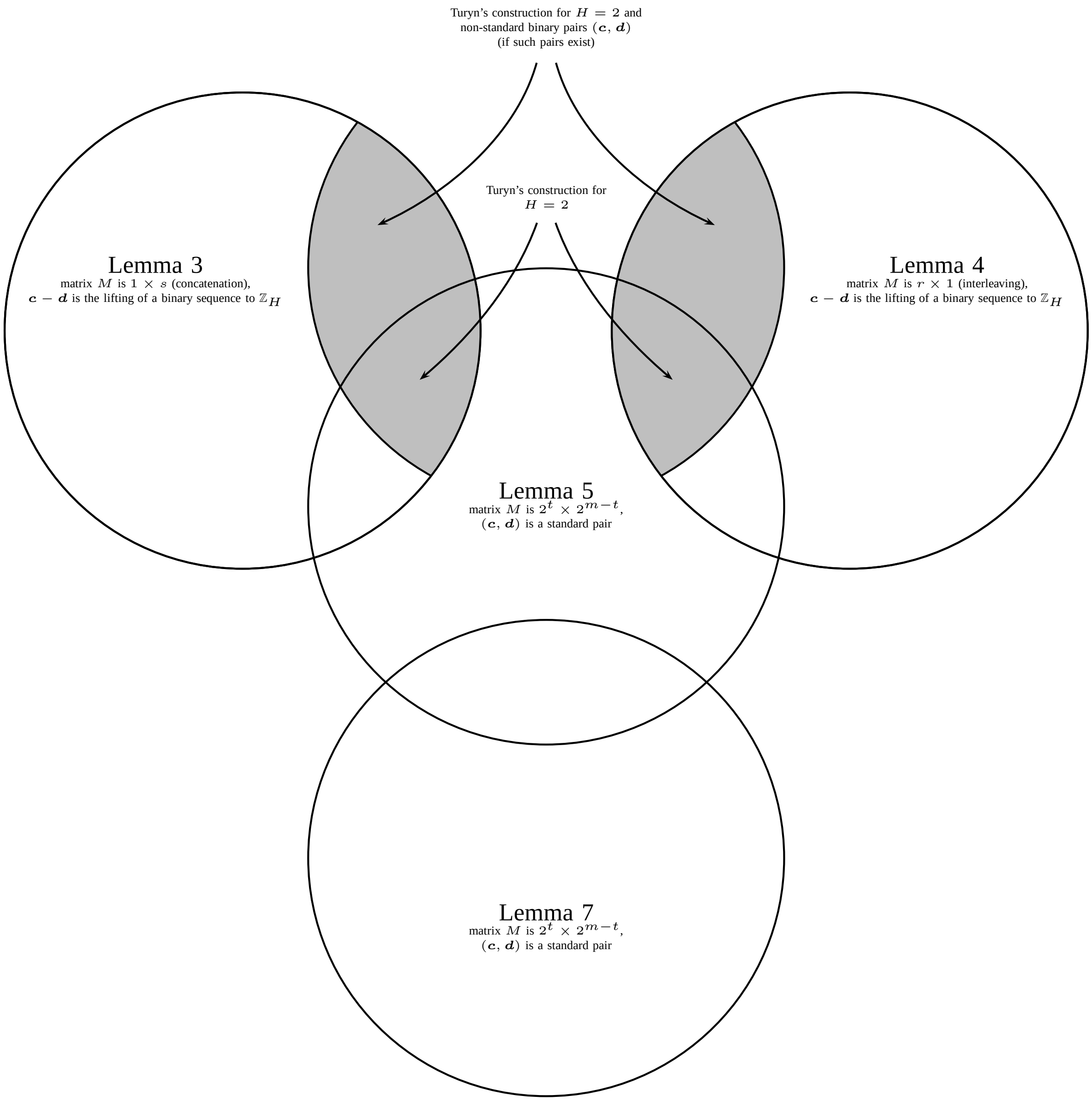


Fig. 1. Venn diagram for constructions of Golay pairs. Annotations describe restrictions on the use of each lemma.

Since AND and XOR generate all possible truth tables, every Boolean function can be expressed uniquely as a linear combination of the above monomials over $\mathbb{Z}_2$, and every generalized Boolean function is a unique linear combination of the monomials over $\mathbb{Z}_H$. The resulting polynomial is called the *algebraic normal form* of f. With the function f we associate a sequence $\boldsymbol{f}$ by listing the values $f(i_1, i_2, \ldots, i_m)$ as $(i_1, i_2, \ldots, i_m)$ ranges over its 2^m values in lexicographic order. In other words, we have $\boldsymbol{f} = (a_0, a_1, \ldots, a_{2^m-1})$ where $a_i = f(i_1, i_2, \ldots, i_m)$. This implies that the sequence associated with the sum $f + g$ of two functions f and g is the componentwise sum of the sequences $\boldsymbol{f}$ and $\boldsymbol{g}$, which we write as $\boldsymbol{f} + \boldsymbol{g}$. Similarly, the sequence associated with the product fg is the componentwise product of $\boldsymbol{f}$ and $\boldsymbol{g}$, which we write as $\boldsymbol{fg}$. We will sometimes write a sequence using a shorthand definition such as $\boldsymbol{f} = x_1x_2$, to mean "$\boldsymbol{f}$ is the sequence associated with the function $f(x_1, \ldots, x_m) = x_1x_2$" (where m will be known from context). For example, when $m = 3$, we have

$$\begin{aligned} f_1(x_1, x_2, x_3) &= x_1 &&= (0, 0, 0, 0, 1, 1, 1, 1), \\ f_2(x_1, x_2, x_3) &= x_2 &&= (0, 0, 1, 1, 0, 0, 1, 1), \\ (f_1f_2)(x_1, x_2, x_3) &= x_1x_2 &&= (0, 0, 0, 0, 0, 0, 1, 1). \end{aligned}$$

We write $\boldsymbol{1}$ and $\boldsymbol{0}$ to denote the all-one and all-zero sequence respectively, whose length will be known from context. Note that some authors use a different labeling convention for the algebraic normal form.

We define a *standard Golay pair* of length 2^m over $\mathbb{Z}_H$ to

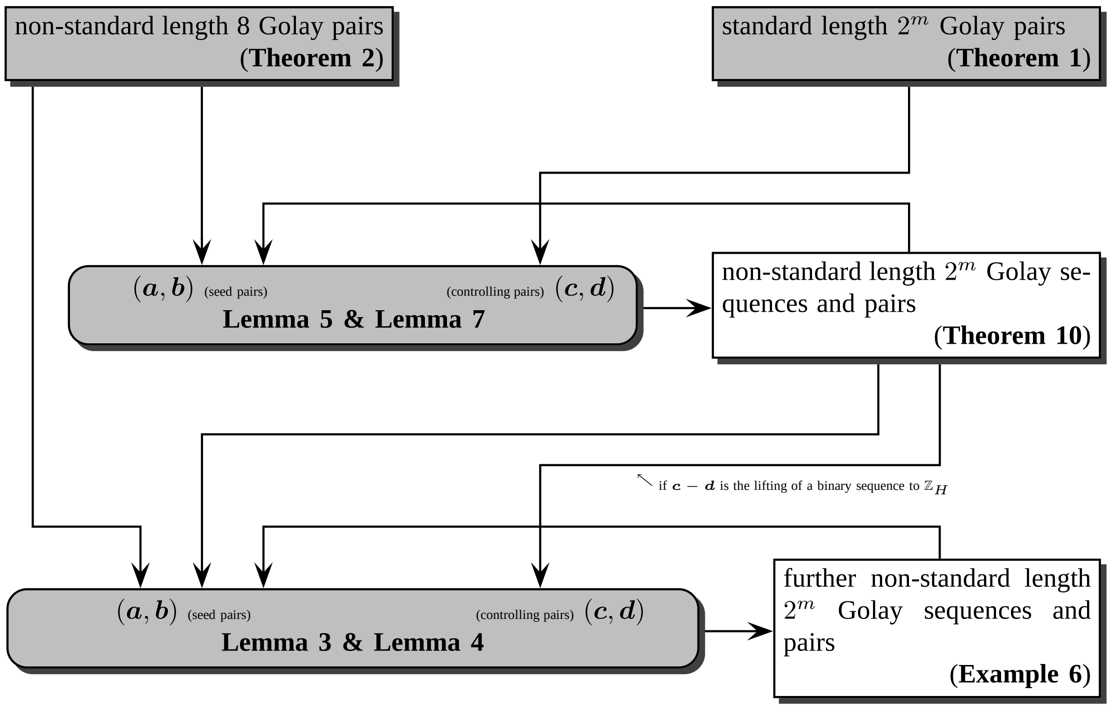


Fig. 2. Flowchart for constructing quaternary length 2^m Golay sequences and pairs (all inputs and outputs are quaternary)

be a pair of sequences $(\boldsymbol{c}, \boldsymbol{d})$ having algebraic normal form

$$\left.\begin{aligned} \boldsymbol{c} &= \frac{H}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} e_k x_k + e_0 \\ \boldsymbol{d} &= \frac{H}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} e_k x_k + e_0' + \frac{H}{2}x_{\pi(1)} \end{aligned}\right\} \tag{1}$$

for some permutation π of $\{1, \ldots, m\}$ and $e_0', e_0, e_1, \ldots, e_m \in \mathbb{Z}_H$, and we define a *standard Golay sequence* to be a member of a standard Golay pair.

Theorem 1. *Let* $\boldsymbol{f} = H/2 \cdot \sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} e_k x_k$, *where* π *is a permutation of* $\{1, 2, \ldots, m\}$ *and* $e_1, e_2, \ldots, e_m \in \mathbb{Z}_H$. *Then the sequence pair*

$$\begin{aligned}&(\boldsymbol{f} + e_0 \cdot \mathbf{1} + H/2 \cdot u(\boldsymbol{x}_{\pi(1)} + \boldsymbol{x}_{\pi(m)}),\\ &\quad \boldsymbol{f} + H/2 \cdot \boldsymbol{x}_{\pi(1)} + e_0' \cdot \mathbf{1} + H/2 \cdot u'(\boldsymbol{x}_{\pi(1)} + \boldsymbol{x}_{\pi(m)}))\end{aligned}$$

is a standard Golay pair of length 2^m *over* $\mathbb{Z}_H$ *for any* $e_0, e_0' \in \mathbb{Z}_H$ *and* $u, u' \in \mathbb{Z}_2$.

The case $H = 2^h$ of Theorem 1 was given by Davis and Jedwab [4, Corollary 5]. Paterson [14] showed that the construction in [4] holds without modification for general (even) H.

Given a sequence $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ of length n over $\mathbb{Z}_H$, we define

$$\boldsymbol{a}^* := (-a_{n-1}, -a_{n-2}, \ldots, -a_0)$$

to be the negative reversal of $\boldsymbol{a}$. (For the associated complex modulated sequence $\boldsymbol{b}$, the sequence $\boldsymbol{b}^*$ is the complex conjugate of the reversal of $\boldsymbol{b}$. If $\boldsymbol{a}$ is a binary sequence, then $\boldsymbol{a}^*$ is just the reversal of $\boldsymbol{a}$ since then $0^* = 0$ and $1^* = 1$.) Since $C_{\boldsymbol{a}^*}(u) \equiv C_{\boldsymbol{a}}(u)$ (see the proof of [5, Lemma 4]), it follows that all sequences in the set

$$E(\boldsymbol{a}) := \{\boldsymbol{a} + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_H\} \cup \{\boldsymbol{a}^* + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_H\}$$

(which has H elements if $\boldsymbol{a}^* = \boldsymbol{a} + c \cdot \mathbf{1}$ for some $c \in \mathbb{Z}_H$, and $2H$ elements otherwise) have identical aperiodic autocorrelation function. Therefore, if $(\boldsymbol{a}, \boldsymbol{b})$ is a Golay pair of length n over $\mathbb{Z}_H$ then so is every element of $E(\boldsymbol{a}) \times E(\boldsymbol{b})$.

Now, using the relations

$$\boldsymbol{x}_i{}^* = \boldsymbol{x}_i - \mathbf{1} \quad \text{and} \quad (\boldsymbol{x}_i\boldsymbol{x}_j)^* = -\boldsymbol{x}_i\boldsymbol{x}_j + \boldsymbol{x}_i + \boldsymbol{x}_j - \mathbf{1}, \tag{2}$$

it follows from (1) that a standard Golay sequence $\boldsymbol{c}$ of length 2^m over $\mathbb{Z}_H$ satisfies

$$\boldsymbol{c}^* = \boldsymbol{c} + H/2 \cdot (\boldsymbol{x}_{\pi(1)} + \boldsymbol{x}_{\pi(m)}) + e \cdot \mathbf{1} \quad \text{for some } e \in \mathbb{Z}_H,$$

so that

$$\begin{aligned} E(\boldsymbol{c}) = \Bigg\{ &\frac{H}{2}\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} e_k x_k + e_0 \\ &+ \frac{H}{2}u(x_{\pi(1)} + x_{\pi(m)}) \mid e_0 \in \mathbb{Z}_H, u \in \mathbb{Z}_2 \Bigg\}. \end{aligned} \tag{3}$$

Therefore Theorem 1 describes the set $E(\boldsymbol{c}) \times E(\boldsymbol{d})$ of Golay pairs derived from a single standard Golay pair $(\boldsymbol{c}, \boldsymbol{d})$.

It is possible that two sequences $\boldsymbol{a}, \boldsymbol{a}'$ of length n over $\mathbb{Z}_H$ have identical aperiodic autocorrelation function, even though $E(\boldsymbol{a}) \neq E(\boldsymbol{a}')$. In this case we say that the pair $(\boldsymbol{a}, \boldsymbol{a}')$ has the *shared autocorrelation property*. Suppose that $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{a}', \boldsymbol{b}')$ are standard Golay pairs, where $E(\boldsymbol{a}) \neq E(\boldsymbol{a}')$ and

$E(\boldsymbol{b}) \neq E(\boldsymbol{b}')$. If the pair $(\boldsymbol{a}, \boldsymbol{a}')$ has the shared autocorrelation property, then so does the pair $(\boldsymbol{b}, \boldsymbol{b}')$; and moreover $(\boldsymbol{a}, \boldsymbol{b}')$ and $(\boldsymbol{a}', \boldsymbol{b})$ both form non-standard Golay pairs by a "cross-over" of their autocorrelation functions, as illustrated in Figure 3. The only known examples of this for $H = 2^h$ can be summarized in Theorem 2.

Theorem 2 ([5]). *For any $u_0, u_1, u_2, u_3 \in \mathbb{Z}_2$ and $k_0, k_1 \in \mathbb{Z}_4$, the length 8 quaternary Golay sequences*

$$\left.\begin{array}{rl} \boldsymbol{a} = & 2(x_1x_2 + x_2x_3) + 2u_0(x_1 + x_3) + 2u_2x_3 \\ & +u_3(x_3 + 2x_2) + k_0 \\ \boldsymbol{b} = & 2(x_1x_2 + x_1x_3) + x_2 + x_3 + 2u_1(x_2 + x_3) \\ & +2u_2x_2 + u_3(x_3 + 2x_2) + k_1 \end{array}\right\}$$

form a non-standard Golay pair, by a cross-over of their autocorrelation functions.

Theorem 2 involves $2 \cdot 2^3 \cdot 4 = 64$ distinct quaternary sequences which form $2 \cdot 2^4 \cdot 4^2 = 512$ non-standard ordered Golay pairs of length 8. [5] demonstrates that all of these Golay pairs can be derived from a single unordered pair of length 8 quaternary Golay sequences having the shared autocorrelation property, for example

$$2(x_1x_2 + x_2x_3) \quad \text{and} \quad 2(x_1x_2 + x_1x_3) + 3x_2 + x_3. \tag{4}$$

For $h > 2$, each quaternary Golay pair in Theorem 2 can be mapped to a Golay pair over $\mathbb{Z}_{2^h}$ having the same complex modulated values, a process known as *lifting* (for example, multiplication of each sequence element by 8 gives a Golay pair over $\mathbb{Z}_{32}$). While these liftings technically provide further examples of standard Golay sequences of length 2^m forming a non-standard Golay pair by a cross-over of their autocorrelation functions, we consider them to be essentially the same as the examples of Theorem 2. By Corollary 2 of [5], a Golay pair $(\boldsymbol{a}, \boldsymbol{b})$ of length n over $\mathbb{Z}_H$ can be mapped to another Golay pair by means of the linear transformation given by adding the sequence $(0, c, 2c, 3c, \dots (n-1)c)$ to both $\boldsymbol{a}$ and $\boldsymbol{b}$ for any $c \in \mathbb{Z}_H$, but we likewise regard these linear transformations of the Golay pairs of Theorem 2 as giving essentially the same pairs.

Our constructions are conveniently described using the matrix notation of Borwein and Ferguson [1]; Paterson [14] used an alternative notation. Let M be an $r \times s$ matrix where each entry is a sequence of length n over $\mathbb{Z}_H$. We regard M as an $r \times sn$ matrix with entries from $\mathbb{Z}_H$, which we read column by column to obtain a new sequence of length rsn over $\mathbb{Z}_H$. Thus the new sequence is the interleaving of r rows, where the entries in each row are the elements in the concatenation of the s sequences in that row. For example, let

$$\boldsymbol{a} = (0, 1, 2, 1)$$
$$\boldsymbol{b} = (0, 1, 0, 3)$$

be quaternary sequences. Then the length 16 quaternary sequence

$$(0, 0, 1, 1, 2, 2, 1, 1, 0, 2, 1, 3, 0, 2, 3, 1)$$

is obtained from the matrix

$$\begin{aligned} M &= \begin{bmatrix} (\boldsymbol{a} + \mathbf{0}) & (\boldsymbol{b} + \mathbf{0}) \\ (\boldsymbol{a} + \mathbf{0}) & (\boldsymbol{b} + 2 \cdot \mathbf{1}) \end{bmatrix} \\ &= \begin{bmatrix} (0, 1, 2, 1) & (0, 1, 0, 3) \\ (0, 1, 2, 1) & (2, 3, 2, 1) \end{bmatrix} \end{aligned}$$

by reading the entries of M column by column. We will present all our constructions in matrix form, using this reading convention for the constructed sequences.

III. Turyn's construction

In this section we review Turyn's construction [16, Lemma 5] in some detail, because of its importance in our constructive framework. We shall illustrate how to convert the construction from the form given by Turyn into the matrix notation described in Section II.

Let $V = \{\boldsymbol{v}^{(j)} \mid 1 \leq j \leq k\}$ be a set of k orthonormal vectors. Turyn defined a *k-symbol δ code of length m* to be a vector sequence $S = (\boldsymbol{s}_0, \boldsymbol{s}_1, \dots, \boldsymbol{s}_{m-1})$, with $\boldsymbol{s}_i \in V$ or $-\boldsymbol{s}_i \in V$ for each i, such that

$$\sum_{i=0}^{m-1-u} \boldsymbol{s}_i \bullet \boldsymbol{s}_{i+u} = 0 \quad \text{for all } u \text{ satisfying } 0 < u < m,$$

where $\bullet$ represents the dot product of vectors. A 2-symbol δ code constructed from the orthonormal "symbols" $\boldsymbol{v}^{(1)} := \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$ and $\boldsymbol{v}^{(2)} := \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$ corresponds to a complex modulated binary Golay pair $(\boldsymbol{c}, \boldsymbol{d})$. This correspondence is given by forming the complex modulated binary sequence $\boldsymbol{c}$ from the first components of the symbols $\pm\boldsymbol{v}^{(1)}$ and $\pm\boldsymbol{v}^{(2)}$ in the vector sequence S, and likewise forming the sequence $\boldsymbol{d}$ from the second components. Thus, the occurrence of $\pm\boldsymbol{v}^{(1)}$ corresponds to $c_i = d_i$, and the occurrence of $\pm\boldsymbol{v}^{(2)}$ corresponds to $c_i \neq d_i$. For example, the 2-symbol δ code

$$\begin{aligned} S &= (+\boldsymbol{v}^{(1)}, +\boldsymbol{v}^{(1)}, +\boldsymbol{v}^{(2)}, -\boldsymbol{v}^{(2)}) \\ &= \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\-1\end{bmatrix}, \begin{bmatrix}-1\\1\end{bmatrix}\right) \end{aligned}$$

corresponds to the sequences $\frac{1}{\sqrt{2}}\boldsymbol{c}$, $\frac{1}{\sqrt{2}}\boldsymbol{d}$, where

$$\boldsymbol{c} = (1, 1, 1, -1),$$
$$\boldsymbol{d} = (1, 1, -1, 1),$$

and $(\boldsymbol{c}, \boldsymbol{d})$ form a complex modulated binary Golay pair (having symbols from $\{1, -1\}$ rather than from $\mathbb{Z}_2$). (The definition of a 2-symbol δ code and its correspondence with a complex modulated binary Golay pair was given prior to [16] by Welti [17], using the name "quaternary code".) Turyn proved there exists a k-symbol δ code of length m_1m_2 for even k, provided that there exists a k-symbol δ code of length m_1 and a 2-symbol δ code of length m_2. In the case $k = 2$, page 320 of [16] (after setting $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}) = (A, -B^*, X, Y)$ and recalling that B^* represents the complex conjugate of the reversal of a complex modulated sequence B) gives the following construction for complex modulated binary Golay pairs. Let $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ be complex modulated binary Golay pairs of length n and s respectively, and let S be

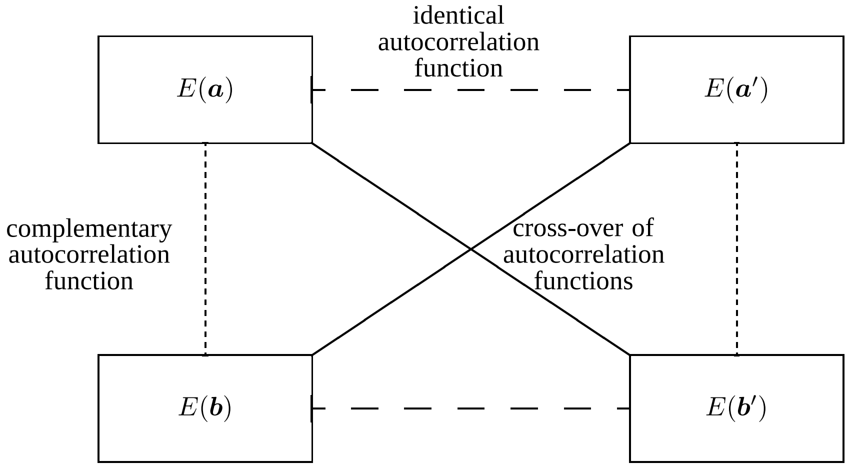


Fig. 3. Cross-over of autocorrelation functions for Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{a}', \boldsymbol{b}')$, where $E(\boldsymbol{a}) \neq E(\boldsymbol{a}')$ and $E(\boldsymbol{b}) \neq E(\boldsymbol{b}')$

the 2-symbol δ code corresponding to $(\boldsymbol{c}, \boldsymbol{d})$ via the symbols $\boldsymbol{v}^{(1)}$ and $\boldsymbol{v}^{(2)}$. Construct a sequence S' consisting of vectors $\pm\boldsymbol{v}^{(3)} := \pm\frac{1}{\boldsymbol{a}\cdot\boldsymbol{a}+\boldsymbol{b}\cdot\boldsymbol{b}}\begin{bmatrix}\boldsymbol{a}\\-\boldsymbol{b}^*\end{bmatrix}$ and $\pm\boldsymbol{v}^{(4)} := \pm\frac{1}{\boldsymbol{a}\cdot\boldsymbol{a}+\boldsymbol{b}\cdot\boldsymbol{b}}\begin{bmatrix}\boldsymbol{b}\\\boldsymbol{a}^*\end{bmatrix}$ by replacing every occurrence of $\pm\boldsymbol{v}^{(1)}$ ($c_i = d_i$) in S with $\pm\boldsymbol{v}^{(3)}$, and every occurrence of $\pm\boldsymbol{v}^{(2)}$ ($c_i \neq d_i$) by $\pm\boldsymbol{v}^{(4)}$. Then S' is a 2-symbol δ code of length sn. For the complex modulated binary example above we get

$$\begin{aligned}S' &= (+\boldsymbol{v}^{(3)}, +\boldsymbol{v}^{(3)}, +\boldsymbol{v}^{(4)}, -\boldsymbol{v}^{(4)})\\ &= \frac{1}{\boldsymbol{a}\cdot\boldsymbol{a}+\boldsymbol{b}\cdot\boldsymbol{b}}\left(\begin{bmatrix}\boldsymbol{a}\\-\boldsymbol{b}^*\end{bmatrix}, \begin{bmatrix}\boldsymbol{a}\\-\boldsymbol{b}^*\end{bmatrix}, \begin{bmatrix}\boldsymbol{b}\\\boldsymbol{a}^*\end{bmatrix}, \begin{bmatrix}-\boldsymbol{b}\\-\boldsymbol{a}^*\end{bmatrix}\right).\end{aligned}$$

Switching to the $\mathbb{Z}_2$ form for binary sequences, this example shows that if $(\boldsymbol{a}, \boldsymbol{b})$ is a binary Golay pair of length n over $\mathbb{Z}_2$ then

$$\boldsymbol{f} = \begin{bmatrix}(\boldsymbol{a}+\boldsymbol{0}) & (\boldsymbol{a}+\boldsymbol{0}) & (\boldsymbol{b}+\boldsymbol{0}) & (\boldsymbol{b}+1\cdot\boldsymbol{1})\end{bmatrix}$$

forms a binary Golay pair of length $4n$ with

$$\boldsymbol{g} = \begin{bmatrix}(\boldsymbol{b}^*+1\cdot\boldsymbol{1}) & (\boldsymbol{b}^*+1\cdot\boldsymbol{1}) & (\boldsymbol{a}^*+\boldsymbol{0}) & (\boldsymbol{a}^*+1\cdot\boldsymbol{1})\end{bmatrix}.$$

Since $\boldsymbol{g}^*+1\cdot\boldsymbol{1}$ has an identical autocorrelation function to $\boldsymbol{g}$, this implies that $\boldsymbol{f}$ also forms a binary Golay pair with

$$\boldsymbol{g}^*+1\cdot\boldsymbol{1} = \begin{bmatrix}(\boldsymbol{a}+\boldsymbol{0}) & (\boldsymbol{a}+1\cdot\boldsymbol{1}) & (\boldsymbol{b}+\boldsymbol{0}) & (\boldsymbol{b}+\boldsymbol{0})\end{bmatrix}.$$

We consider it easier to work with the pair $(\boldsymbol{f}, \boldsymbol{g}^*+1\cdot\boldsymbol{1})$ than the pair $(\boldsymbol{f}, \boldsymbol{g})$ suggested by [16]. The reason is that $\boldsymbol{f}$ and $\boldsymbol{g}^*+1\cdot\boldsymbol{1}$ are both obtained through concatenation of the sequences (regarded as blocks) of the binary Golay pair $(\boldsymbol{a}, \boldsymbol{b})$. Moreover the sequences $\boldsymbol{c}$ and $\boldsymbol{d}^*$ of length s over $\mathbb{Z}_2$ can be recognized in the forms for $\boldsymbol{f}$ and $\boldsymbol{g}^*+1\cdot\boldsymbol{1}$, while the placement of $\boldsymbol{a}$ or $\boldsymbol{b}$ in $\boldsymbol{f}$ and $\boldsymbol{g}^*+1\cdot\boldsymbol{1}$ depends only on the positions at which $\boldsymbol{c}$ and $\boldsymbol{d}$ coincide. This result is a key construction for Golay pairs which we will present in more general form in Lemma 3.

The description on page 320 of [16] involves a non-standard interpretation of the Kronecker product. With the standard Kronecker product, the constructed sequences $\boldsymbol{f}$ and $\boldsymbol{g}^*+1\cdot\boldsymbol{1}$ involve the interleaving rather than the concatenation of sequences. We will present this variation in more general form in Lemma 4. We regard both interpretations (namely the case $H = 2$ of Lemmas 3 and 4) as "Turyn's construction".

Page 320 of [16] contains, in addition to the formula explained above for $k = 2$, an algorithmic description of the construction for k-symbol δ codes for general k. In the cases $k > 2$ these codes do not correspond to complex modulated Golay pairs, but we found the algorithmic description useful in determining the form of Lemmas 3 and 4 for general H.

IV. Constructive Framework

In this section we develop variations on Turyn's construction, in which Golay pairs $(\boldsymbol{c}, \boldsymbol{d})$ are used to control the creation of new Golay pairs $(\boldsymbol{f}, \boldsymbol{g})$ from an arbitrary Golay pair $(\boldsymbol{a}, \boldsymbol{b})$. The constuctions will be presented using the matrix notation introduced in Section II. The controlling pair $(\boldsymbol{c}, \boldsymbol{d})$ need not be binary; it is sufficient that $\boldsymbol{c}-\boldsymbol{d}$ is the lifting of a binary sequence to $\mathbb{Z}_H$. As throughout, H is an even positive integer and ξ is a primitive H-th root of unity.

A. Two variations on Turyn's construction

In this subsection we present two variations on Turyn's construction. We begin with the first variation, in which the matrices determining $\boldsymbol{f}$ and $\boldsymbol{g}$ have size $1 \times s$ so that $\boldsymbol{f}$ and $\boldsymbol{g}$ are each the concatenation of s sequences.

Lemma 3. *Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Golay pair of length n over $\mathbb{Z}_H$. Let $\boldsymbol{c} = (c_0, c_1, \ldots, c_{s-1})$ and $\boldsymbol{d} = (d_0, d_1, \ldots, d_{s-1})$ be a Golay pair of length s over $\mathbb{Z}_H$ for which $\boldsymbol{c}-\boldsymbol{d}$ is the lifting of a binary sequence to $\mathbb{Z}_H$. Define length n sequences*

$$\delta(i) := \begin{cases}\boldsymbol{a}+c_i\cdot\boldsymbol{1} & \text{if } c_i = d_i\\ \boldsymbol{b}+c_i\cdot\boldsymbol{1} & \text{if } c_i \neq d_i,\end{cases}$$

$$\delta'(i) := \begin{cases}\boldsymbol{a}+d_i^*\cdot\boldsymbol{1} & \text{if } d_i^* \neq c_i^*\\ \boldsymbol{b}+d_i^*\cdot\boldsymbol{1} & \text{if } d_i^* = c_i^*,\end{cases}$$

where $d_i^* := (\boldsymbol{d}^*)_i$. Then the sequence $\boldsymbol{f}$ obtained from the $1 \times s$ matrix

$$M := \begin{bmatrix}\delta(0) & \delta(1) & \cdots & \delta(s-1)\end{bmatrix}$$

forms a Golay pair of length sn over $\mathbb{Z}_H$ with the sequence $\boldsymbol{g}$ obtained from the $1 \times s$ matrix

$$M' := \begin{bmatrix} \delta'(0) & \delta'(1) & \cdots & \delta'(s-1) \end{bmatrix}.$$

Proof: $\boldsymbol{f}$ and $\boldsymbol{g}$ are clearly sequences of length sn over $\mathbb{Z}_H$. Let $A(x)$, $B(x)$, $C(x)$, $D(x)$, $C^*(x)$, and $D^*(x)$ denote the generating function associated with $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$, $\boldsymbol{c}^*$, and $\boldsymbol{d}^*$, respectively. For each i, by assumption $d_i = c_i$ or $d_i = c_i + H/2$. Therefore the coefficient of x^i in $C(x)+D(x)$ is $2\xi^{c_i}$ if $c_i = d_i$ and 0 otherwise; and the coefficient of x^i in $C(x) - D(x)$ is $2\xi^{c_i}$ if $c_i \neq d_i$ and 0 otherwise. So the generating function associated with $\boldsymbol{f}$ is

$$F(x) = A(x)\,\frac{C(x^n) + D(x^n)}{2} + B(x)\,\frac{C(x^n) - D(x^n)}{2},$$

and similarly the generating function associated with $\boldsymbol{g}$ is

$$G(x) = A(x)\,\frac{D^*(x^n) - C^*(x^n)}{2} + B(x)\,\frac{D^*(x^n) + C^*(x^n)}{2}.$$

But for any generating functions $Y(x), Z(x)$ associated with sequences of the same length, straightforward manipulation shows that $Y^*(x)\overline{Z^*(x^{-1})} = \overline{Y(x^{-1})}Z(x)$. It follows that

$$F(x)\overline{F(x^{-1})} + G(x)\overline{G(x^{-1})} = 2sn,$$

so $(\boldsymbol{f}, \boldsymbol{g})$ form a Golay pair. ∎

For example, the quaternary sequences

$$\left.\begin{array}{rcl} \boldsymbol{a} &=& (0,1,2,1) \\ \boldsymbol{b} &=& (0,1,0,3) \end{array}\right\} \tag{5}$$

form a Golay pair, and the quaternary sequences

$$\left.\begin{array}{rl} \boldsymbol{c} &= (0,0,0,2) \\ \boldsymbol{d} &= (0,0,2,0) \end{array}\right\} \tag{6}$$

form a Golay pair for which $\boldsymbol{c} - \boldsymbol{d} = (0,0,2,2)$ is the lifting of a binary sequence to $\mathbb{Z}_4$. By Lemma 3, the sequences

$$\boldsymbol{f} = (0,1,2,1,0,1,2,1,0,1,0,3,2,3,2,1)$$
$$\boldsymbol{g} = (0,1,2,1,2,3,0,3,0,1,0,3,0,1,0,3)$$

obtained from the respective matrices

$$M = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{b}+\mathbf{0}) & (\boldsymbol{b}+2\cdot\mathbf{1}) \end{bmatrix}$$
$$M' = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+2\cdot\mathbf{1}) & (\boldsymbol{b}+\mathbf{0}) & (\boldsymbol{b}+\mathbf{0}) \end{bmatrix}$$

then form a quaternary Golay pair of length 16.

In the special case $s = 2$ and $\boldsymbol{c} = (0, H/2)$, $\boldsymbol{d} = (0,0)$ of Lemma 3, the constructed sequences are $\boldsymbol{f} = \begin{bmatrix} \boldsymbol{a} & (\boldsymbol{b} + H/2\cdot\mathbf{1}) \end{bmatrix}$ and $\boldsymbol{g} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} \end{bmatrix}$. This is Golay's concatenation construction [8, (9)].

We next present the second variation on Turyn's construction, in which the matrices determining $\boldsymbol{f}$ and $\boldsymbol{g}$ have size $r \times 1$ so that $\boldsymbol{f}$ and $\boldsymbol{g}$ are each the interleaving of r sequences.

Lemma 4. *Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Golay pair of length n over $\mathbb{Z}_H$. Let $\boldsymbol{c} = (c_0, c_1, \ldots, c_{r-1})$ and $\boldsymbol{d} = (d_0, d_1, \ldots, d_{r-1})$ be a Golay pair of length r over $\mathbb{Z}_H$ for which $\boldsymbol{c} - \boldsymbol{d}$ is the lifting of a binary sequence to $\mathbb{Z}_H$. Define length n sequences*

$$\delta(i) := \begin{cases} \boldsymbol{a} + c_i \cdot \mathbf{1} & \text{if } c_i = d_i \\ \boldsymbol{b} + c_i \cdot \mathbf{1} & \text{if } c_i \neq d_i, \end{cases}$$

$$\delta'(i) := \begin{cases} \boldsymbol{a} + d_i^* \cdot \mathbf{1} & \text{if } d_i^* \neq c_i^* \\ \boldsymbol{b} + d_i^* \cdot \mathbf{1} & \text{if } d_i^* = c_i^*, \end{cases}$$

where $d_i^* := (\boldsymbol{d}^*)_i$. Then the sequence $\boldsymbol{f}$ obtained from the $r \times 1$ matrix

$$M := \begin{bmatrix} \delta(0) \\ \delta(1) \\ \vdots \\ \delta(r-1) \end{bmatrix}$$

forms a Golay pair of length rn over $\mathbb{Z}_H$ with the sequence $\boldsymbol{g}$ obtained from the $r \times 1$ matrix

$$M' := \begin{bmatrix} \delta'(0) \\ \delta'(1) \\ \vdots \\ \delta'(r-1) \end{bmatrix}.$$

Proof: The proof is similar to that of Lemma 3. The generating functions associated with $\boldsymbol{f}$ and $\boldsymbol{g}$ are

$$F(x) = A(x^r)\,\frac{C(x) + D(x)}{2} + B(x^r)\,\frac{C(x) - D(x)}{2}$$
$$G(x) = A(x^r)\,\frac{D^*(x) - C^*(x)}{2} + B(x^r)\,\frac{D^*(x) + C^*(x)}{2},$$

respectively, and these functions form a complementary pair. ∎

For example, consider again the Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ in (5) and (6) respectively. By Lemma 4, the sequences

$$\boldsymbol{f'} = (0,0,0,2,1,1,1,3,2,2,0,2,1,1,3,1)$$
$$\boldsymbol{g'} = (0,2,0,0,1,3,1,1,2,0,0,0,1,3,3,3)$$

obtained from the respective matrices

$$M = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) \\ (\boldsymbol{a}+\mathbf{0}) \\ (\boldsymbol{b}+\mathbf{0}) \\ (\boldsymbol{b}+2\cdot\mathbf{1}) \end{bmatrix} = \begin{bmatrix} (0,1,2,1) \\ (0,1,2,1) \\ (0,1,0,3) \\ (2,3,2,1) \end{bmatrix}$$
$$M' = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) \\ (\boldsymbol{a}+2\cdot\mathbf{1}) \\ (\boldsymbol{b}+\mathbf{0}) \\ (\boldsymbol{b}+\mathbf{0}) \end{bmatrix} = \begin{bmatrix} (0,1,2,1) \\ (2,3,0,3) \\ (0,1,0,3) \\ (0,1,0,3) \end{bmatrix}$$

form a quaternary Golay pair of length 16.

In the special case $r = 2$ and $\boldsymbol{c} = (0, H/2)$, $\boldsymbol{d} = (0,0)$ of Lemma 4, the constructed sequence $\boldsymbol{f}$ is the elementwise interleaving of $\boldsymbol{a}$ and $\boldsymbol{b} + H/2 \cdot \mathbf{1}$, and $\boldsymbol{g}$ is the elementwise interleaving of $\boldsymbol{a}$ and $\boldsymbol{b}$. This is Golay's interleaving construction [8, (10)].

We will refer to the pair $(\boldsymbol{a}, \boldsymbol{b})$ of Lemmas 3 and 4 (and later Lemmas 5 and 7) as the *seed pair*, and to $(\boldsymbol{c}, \boldsymbol{d})$ as the *controlling pair*. To emphasize that Lemmas 3 and 4 are not restricted to Golay pairs whose length is a power of 2, for example let $(\boldsymbol{a},\boldsymbol{b})$ be the quaternary Golay pair of length 3 with $\boldsymbol{a}=(0,0,2)$ and $\boldsymbol{b}=(0,1,0)$, and let $(\boldsymbol{c},\boldsymbol{d})$ be the quaternary Golay pair of length 6 with $\boldsymbol{c}=(0,0,2,0,1,0)$ and $\boldsymbol{d}=(0,0,2,2,3,2)$. Then the sequence $\boldsymbol{f}$ given by

$$[(\boldsymbol{a}+\mathbf{0})\ \ (\boldsymbol{a}+\mathbf{0})\ \ (\boldsymbol{a}+2\cdot\mathbf{1})\ \ (\boldsymbol{b}+\mathbf{0})\ \ (\boldsymbol{b}+1\cdot\mathbf{1})\ \ (\boldsymbol{b}+\mathbf{0})]$$
$$=(0,0,2,0,0,2,2,2,0,0,1,0,1,2,1,0,1,0)$$

is a quaternary Golay sequence of length 18 by Lemma 3, and the sequence $\boldsymbol{f}'$ given by

$$\begin{bmatrix}(\boldsymbol{a}+\mathbf{0})\\(\boldsymbol{a}+\mathbf{0})\\(\boldsymbol{a}+2\cdot\mathbf{1})\\(\boldsymbol{b}+\mathbf{0})\\(\boldsymbol{b}+1\cdot\mathbf{1})\\(\boldsymbol{b}+\mathbf{0})\end{bmatrix}=(0,0,2,0,1,0,0,0,2,1,2,1,2,2,0,0,1,0)$$

is a quaternary Golay sequence of length 18 by Lemma 4. Since there are binary Golay pairs of length 2, 10 [8] and 26 [9], by repeated application of Lemmas 3 and 4 we can similarly construct quaternary Golay pairs for a variety of lengths that are not powers of 2, for example length $3\cdot 10^3\cdot 2^4$ or $6\cdot 26^2\cdot 10\cdot 2^2$.

Lemma 3 can easily be modified to the case of complex modulated sequences $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}$ of arbitrary complex numbers, using the complex modulated definition of aperiodic autocorrelation function and generating function mentioned in Section II. The condition on $\boldsymbol{c},\boldsymbol{d}$ is that, for each i, $c_i=d_i$ or $c_i=-d_i$. Each $\delta(i)$ is then defined to be $c_i\boldsymbol{a}$ if $c_i=d_i$, and $c_i\boldsymbol{b}$ if $c_i=-d_i$; the definition of $\delta'(i)$ is similar. The rest of the proof resembles that of Lemma 3, and in particular the generating functions $F(x)$ and $G(x)$ are given by the same equations. Lemma 4 can likewise be modified for sequences of arbitrary complex numbers.

The construction of Lemmas 3 and 4 is governed by matrices consisting of a single row and a single column respectively. In Lemma 5 we shall present a further variation of Turyn's construction in which the matrices have the more general size $2^t\times 2^{m-t}$ for any integer t satisfying $0\le t\le m$. In exchange for this additional freedom, the controlling Golay pair $(\boldsymbol{c},\boldsymbol{d})$ will be restricted to be standard (and, in particular, of length 2^m).

B. Budišin's construction

In this subsection we describe Budišin's iterative construction for a standard Golay pair from an initial Golay pair of length 1, in preparation for the proof of Lemma 5.

Let $\boldsymbol{c}=(c_0,c_1,\ldots,c_{2^m-1})$ and $\boldsymbol{d}=(d_0,d_1,\ldots,d_{2^m-1})$ be a standard Golay pair of length 2^m over $\mathbb{Z}_H$, satisfying (1) for some permutation π of $\{1,\ldots,m\}$ and $e_0',e_0,e_1,\ldots,e_m\in\mathbb{Z}_H$; assume by suitable choice of e_0' that $c_0=d_0^*$. Budišin's construction produces the standard Golay pair $(\boldsymbol{c},\boldsymbol{d}^*)$ of length 2^m iteratively from the initial Golay pair $((c_0),(c_0))$ of length 1. At step 0, form the complementary function pair

$$C^{(0)}(x):=\xi^{c_0}$$
$$D^{*(0)}(x):=\xi^{c_0}.$$

At step $\ell+1$ (for $0\le\ell<m$), construct the complementary function pair

$$\left.\begin{aligned}C^{(\ell+1)}(x)&:=C^{(\ell)}(x)+\xi^{e_{\pi(\ell+1)}}D^{*(\ell)}(x)\,x^{2^{m-\pi(\ell+1)}}\\D^{*(\ell+1)}(x)&:=C^{(\ell)}(x)-\xi^{e_{\pi(\ell+1)}}D^{*(\ell)}(x)\,x^{2^{m-\pi(\ell+1)}}\end{aligned}\right\}. \tag{7}$$

Then $C^{(m)}(x)$ and $D^{*(m)}(x)$ are the generating function for $\boldsymbol{c}$ and $\boldsymbol{d}^*$ respectively.

We can view the sequence elements of $\boldsymbol{c}$ and $\boldsymbol{d}^*$ as being filled in at step $\ell+1$ to form sequences $\boldsymbol{c}^{(\ell+1)}$ and $\boldsymbol{d}^{*(\ell+1)}$ corresponding to $C^{(\ell+1)}(x)$ and $D^{*(\ell+1)}(x)$ respectively. In this process the sequence elements of $\boldsymbol{c}$ do not change once filled in, whereas the sequence elements of $\boldsymbol{d}^*$ are finalized only at the last step. (In [2], the sequence $(\xi^{e_{\pi(1)}},\ldots,\xi^{e_{\pi(m)}})$ is called the W-vector, and the sequence $(m-\pi(1),\ldots,m-\pi(m))$ is called the permutation vector P. We have modified the initial complementary function pair trivially, from the pair $((1),(1))$ specified in [2] to the pair $((\xi^{c_0}),(\xi^{c_0}))$.)

For example, take $H=4$, $m=4$, $(\pi(1),\pi(2),\pi(3),\pi(4))=(3,4,1,2)$, $(e_1,e_2,e_3,e_4)=(3,0,2,1)$, and $(e_0,e_0')=(0,2)$ in (1) to give the standard length 16 quaternary Golay pair

$$\begin{aligned}\boldsymbol{c}&=2(x_3x_4+x_4x_1+x_1x_2)+3x_1+2x_3+x_4\\&=(0,1,2,1,0,1,2,1,3,2,1,2,1,0,3,0)\\\boldsymbol{d}&=2(x_3x_4+x_4x_1+x_1x_2)+3x_1+x_4+2\\&=(2,3,2,1,2,3,2,1,1,0,1,2,3,2,3,0)\end{aligned}$$

that satisfies $c_0=d_0^*$. We shall now construct the pair $(\boldsymbol{c},\boldsymbol{d}^*)$ using Budišin's construction. At step $\ell+1$ we add to (and subtract from) $C^{(\ell)}(x)$ a "shift" of the term $\xi^{e_{\pi(\ell+1)}}D^{*(\ell)}(x)$ by $x^{2^{m-\pi(\ell+1)}}$, according to (7). Using the values $(\xi^{e_{\pi(1)}},\xi^{e_{\pi(2)}},\xi^{e_{\pi(3)}},\xi^{e_{\pi(4)}})=(\xi^2,\xi^1,\xi^3,\xi^0)$ and $(x^{2^{m-\pi(1)}},x^{2^{m-\pi(2)}},x^{2^{m-\pi(3)}},x^{2^{m-\pi(4)}})=(x^2,x^1,x^8,x^4)$, we obtain

$$\begin{aligned}
\boldsymbol{c}^{(0)}&=(0\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{d}^{*(0)}&=(0\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{c}^{(1)}&=(0\ \cdot\ 2\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{d}^{*(1)}&=(0\ \cdot\ 0\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{c}^{(2)}&=(0\ 1\ 2\ 1\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{d}^{*(2)}&=(0\ 3\ 2\ 3\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{c}^{(3)}&=(0\ 1\ 2\ 1\ \cdot\ \cdot\ \cdot\ \cdot\ 3\ 2\ 1\ 2\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{d}^{*(3)}&=(0\ 1\ 2\ 1\ \cdot\ \cdot\ \cdot\ \cdot\ 1\ 0\ 3\ 0\ \cdot\ \cdot\ \cdot\ \cdot)\\
\boldsymbol{c}=\boldsymbol{c}^{(4)}&=(0\ 1\ 2\ 1\ 0\ 1\ 2\ 1\ 3\ 2\ 1\ 2\ 1\ 0\ 3\ 0)\\
\boldsymbol{d}^*=\boldsymbol{d}^{*(4)}&=(0\ 1\ 2\ 1\ 2\ 3\ 0\ 3\ 3\ 2\ 1\ 2\ 3\ 2\ 1\ 2).
\end{aligned}$$

C. A third variation on Turyn's construction

In this subsection we give a third variation on Turyn's construction, Lemma 5, in which the matrices determining the constructed Golay pair $(\boldsymbol{f},\boldsymbol{g})$ have size $2^t\times 2^{m-t}$ for any integer t satisfying $0\le t\le m$. To prove the correctness of this construction we shall modify Budišin's iterative construction of Section IV-B, replacing the initial Golay pair $((c_0),(c_0))$ by an arbitrary Golay pair $(\boldsymbol{a}+c_0\cdot\mathbf{1},\boldsymbol{b}+c_0\cdot\mathbf{1})$. The proof indicates that Budišin's construction can itself be recast to resemble Turyn's construction. (At the end of this subsection we shall show that the conditions in Lemma 5 involving the variable $i_{\pi(1)}$ have an alternative formulation in terms of the sequence elements c_i and d_i, similar to those appearing in Lemmas 3 and 4.)

We firstly illustrate the construction by means of an example with $m = 4$ and $t = 2$, which is based on the example given in Section IV-B. This example is intended to be read in conjunction with the proof of Lemma 5:

$$M^{(0)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M'^{(0)} = \begin{bmatrix} (\boldsymbol{b}+\mathbf{0}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M^{(1)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M'^{(1)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+\mathbf{0}) & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M^{(2)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M'^{(2)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}+3\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+3\cdot\mathbf{1}) & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M^{(3)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & (\boldsymbol{a}+3\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}+2\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot \end{bmatrix}$$

$$M'^{(3)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}+\mathbf{0}) & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}+3\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}+\mathbf{0}) & \cdot \end{bmatrix}$$

$$M^{(4)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+3\cdot\mathbf{1}) & (\boldsymbol{a}+1\cdot\mathbf{1}) \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{a}+2\cdot\mathbf{1}) & (\boldsymbol{a}+\mathbf{0}) \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+3\cdot\mathbf{1}) \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+\mathbf{0}) \end{bmatrix}$$

$$M'^{(4)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+2\cdot\mathbf{1}) & (\boldsymbol{a}+3\cdot\mathbf{1}) & (\boldsymbol{a}+3\cdot\mathbf{1}) \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{a}+3\cdot\mathbf{1}) & (\boldsymbol{a}+2\cdot\mathbf{1}) & (\boldsymbol{a}+2\cdot\mathbf{1}) \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+\mathbf{0}) & (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+1\cdot\mathbf{1}) \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+3\cdot\mathbf{1}) & (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+2\cdot\mathbf{1}) \end{bmatrix},$$

and $M = M^{(4)}$ and $M' = M'^{(4)}$.

Lemma 5. *Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Golay pair of length n over $\mathbb{Z}_H$. Let $\boldsymbol{c} = (c_0, c_1, \ldots, c_{2^m-1})$ and $\boldsymbol{d} = (d_0, d_1, \ldots, d_{2^m-1})$ be a standard Golay pair of length 2^m over $\mathbb{Z}_H$, satisfying (1) for some permutation π of $\{1, \ldots, m\}$. Write $(i_1, i_2, \ldots, i_m)$ for the binary representation of the integer i in the range $0 \le i < 2^m$, and define length n sequences*

$$\delta(i) := \begin{cases} \boldsymbol{a} + c_i \cdot \mathbf{1} & \text{if } i_{\pi(1)} = 0 \\ \boldsymbol{b} + c_i \cdot \mathbf{1} & \text{if } i_{\pi(1)} = 1, \end{cases}$$

$$\delta'(i) := \begin{cases} \boldsymbol{a} + d_i^* \cdot \mathbf{1} & \text{if } i_{\pi(1)} = 0 \\ \boldsymbol{b} + d_i^* \cdot \mathbf{1} & \text{if } i_{\pi(1)} = 1. \end{cases}$$

Then, for any integer t satisfying $0 \le t \le m$, the sequence $\boldsymbol{f}$ obtained from the $2^t \times 2^{m-t}$ matrix

$$M := \begin{bmatrix} \delta(0) & \delta(2^t) & \cdots & \delta(2^m - 2^t) \\ \delta(1) & \delta(2^t+1) & & \\ \vdots & & \ddots & \vdots \\ \delta(2^t - 1) & \delta(2 \cdot 2^t - 1) & \cdots & \delta(2^m - 1) \end{bmatrix}$$

forms a Golay pair of length $2^m n$ over $\mathbb{Z}_H$ with the sequence $\boldsymbol{g}$ obtained from the $2^t \times 2^{m-t}$ matrix

$$M' := \begin{bmatrix} \delta'(0) & \delta'(2^t) & \cdots & \delta'(2^m - 2^t) \\ \delta'(1) & \delta'(2^t+1) & & \\ \vdots & & \ddots & \vdots \\ \delta'(2^t - 1) & \delta'(2 \cdot 2^t - 1) & \cdots & \delta'(2^m - 1) \end{bmatrix}.$$

Proof: We may assume that $c_0 = d_0^*$, by replacing $\boldsymbol{d}$ by $\boldsymbol{d} + e \cdot \mathbf{1}$ for some $e \in \mathbb{Z}_H$ if necessary: the pair $(\boldsymbol{c}, \boldsymbol{d} + e \cdot \mathbf{1})$ is still a standard Golay pair, and the constructed pair $(\boldsymbol{f}, \boldsymbol{g} - e \cdot \mathbf{1})$ is a Golay pair if and only if $(\boldsymbol{f}, \boldsymbol{g})$ is. Let $A(x)$, $B(x)$, $F(x)$, and $G(x)$ denote the generating function associated with $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{f}$, and $\boldsymbol{g}$, respectively. We shall construct the Golay pair $(\boldsymbol{f}, \boldsymbol{g})$ iteratively from the initial Golay pair $(\boldsymbol{a} + c_0 \cdot \mathbf{1}, \boldsymbol{b} + c_0 \cdot \mathbf{1})$, by mimicking Budišin's construction of Section IV-B for the standard Golay pair $(\boldsymbol{c}, \boldsymbol{d}^*)$ from the initial Golay pair $((c_0), (c_0))$ of length 1.

We can view the entries of the matrices M and M' (corresponding to the sequences $\boldsymbol{f}$ and $\boldsymbol{g}$ respectively) as being filled in by reference to (7). At step $\ell + 1$ (for $0 \le \ell < m$) we fill in all the sequences $\delta(i)$ and $\delta'(i)$ for which the coefficient of x^i in $C^{(\ell+1)}(x)$ (and therefore in $D^{*(\ell+1)}(x)$) is nonzero, to form matrices $M^{(\ell+1)}$ and $M'^{(\ell+1)}$. The entries for M do not change once filled in, whereas the entries for M' are finalized only at the last step. We shall show that the generating functions $F^{(\ell+1)}(x)$ and $G^{(\ell+1)}(x)$ corresponding to $M^{(\ell+1)}$ and $M'^{(\ell+1)}$ form a complementary function pair, and complete the proof by showing that $F^{(m)}(x) = F(x)$ and $G^{(m)}(x) = G(x)$.

At step 0 we set

$$F^{(0)}(x) := A(x^{2^t}) \cdot \xi^{c_0}$$
$$G^{(0)}(x) := B(x^{2^t}) \cdot \xi^{c_0}.$$

Since $(\boldsymbol{a} + c_0 \cdot \mathbf{1}, \boldsymbol{b} + c_0 \cdot \mathbf{1})$ is a Golay pair, $(F^{(0)}(x), G^{(0)}(x))$ is a complementary function pair. At step 1 we mimic the operations that yielded $C^{(1)}(x)$ and $D^{*(1)}(x)$ in Section IV-B, by adding to (and subtracting from) $F^{(0)}(x)$ an appropriate "shift" of the term $\xi^{e_{\pi(1)}} G^{(0)}(x)$ by some x^i. The resulting functions are $F^{(1)}(x)$ and $G^{(1)}(x)$. The shift by $x^{2^{m-\pi(1)}}$ in the construction of $C^{(1)}(x)$ and $D^{*(1)}(x)$ corresponds to a shift to the entry in row k and column j of the matrices M

and M' for which $2^{m-\pi(1)} = 2^t j + k$, and the adjusted shift for $F^{(1)}(x)$ and $G^{(1)}(x)$ is $x^{2^t nj+k}$ since each matrix entry contains a sequence of length n. By construction of $\boldsymbol{c}$ and $\boldsymbol{d}^*$ from (7), $F^{(0)}(x)$ and $\xi^{e_{\pi(1)}} G^{(0)}(x) x^{2^t nj+k}$ have no common support, and we obtain the two generating functions

$$F^{(1)}(x) := F^{(0)}(x) + \xi^{e_{\pi(1)}} G^{(0)}(x) x^{2^t nj+k}$$
$$G^{(1)}(x) := F^{(0)}(x) - \xi^{e_{\pi(1)}} G^{(0)}(x) x^{2^t nj+k}.$$

Routine calculation shows that

$$\begin{aligned} &F^{(1)}(x)\overline{F^{(1)}(x^{-1})} + G^{(1)}(x)\overline{G^{(1)}(x^{-1})} \\ &= \;\; 2\left(F^{(0)}(x)\overline{F^{(0)}(x^{-1})} + G^{(0)}(x)\overline{G^{(0)}(x^{-1})}\right), \end{aligned}$$

and so $(F^{(1)}(x), G^{(1)}(x))$ is a complementary function pair. Since bit $\pi(1)$ of 0 is 0, and bit $\pi(1)$ of $2^{m-\pi(1)}$ is 1, we have

$$\delta(0) = \boldsymbol{a} + c_0 \cdot \mathbf{1}$$
$$\delta(2^{m-\pi(1)}) = \boldsymbol{b} + c_{2^{m-\pi(1)}} \cdot \mathbf{1}$$

by definition of $\delta(i)$. Thus, $\delta(0)$ matches $A(x^{2^t}) \cdot \xi^{c_0} = F^{(0)}(x)$ in $F^{(1)}(x)$, and $\delta(2^{m-\pi(1)})$ matches the term $B(x^{2^t}) \cdot \xi^{c_{2^{m-\pi(1)}}} = B(x^{2^t}) \cdot \xi^{c_0+e_{\pi(1)}} = \xi^{e_{\pi(1)}} G^{(0)}(x)$ in $F^{(1)}(x)$ (using the case $\ell = 0$ of (7) to show that $c_0 + e_{\pi(1)} = c_{2^{m-\pi(1)}}$). The iterative definition of $F^{(1)}(x)$ therefore coincides with that obtained directly from δ.

This gives the pattern for an inductive proof. The inductive hypothesis is that, after step ℓ, $F^{(\ell)}(x)$ and $G^{(\ell)}(x)$ form a complementary function pair; the iterative definition of $F^{(\ell)}(x)$ coincides with that obtained directly from δ; and the placement of $A(x^{2^t})$ and $B(x^{2^t})$ in $G^{(\ell)}(x)$ matches the placement of $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively in the definition of δ. Define j and k in the range $0 \le j < 2^{m-t}$ and $0 \le k < 2^t$ so that $2^{m-\pi(\ell+1)} = 2^t j + k$. Then $F^{(\ell)}(x)$ and $\xi^{e_{\pi(\ell+1)}} G^{(\ell)}(x) x^{2^t nj+k}$ have no common support and

$$F^{(\ell+1)}(x) = F^{(\ell)}(x) + \xi^{e_{\pi(\ell+1)}} G^{(\ell)}(x) x^{2^t nj+k}$$
$$G^{(\ell+1)}(x) = F^{(\ell)}(x) - \xi^{e_{\pi(\ell+1)}} G^{(\ell)}(x) x^{2^t nj+k}$$

form a complementary function pair, by a similar argument to that used above.

For any i in the range $0 \le i < 2^m$, suppose $\delta(i)$ has been filled from matrix M at step $\ell + 1$. Therefore, bit $\pi(1)$ in the binary representation of $m - \pi(\ell+1)$ must be zero, and $m - \pi(1) \ne m - \pi(\ell+1)$. Hence $(i + 2^{m-\pi(\ell+1)})_{\pi(1)} = i_{\pi(1)}$, and by the inductive hypothesis the iterative definition of $F^{(\ell+1)}(x)$ coincides with that obtained directly from δ, and the placement of $A(x^{2^t})$ and $B(x^{2^t})$ in the iterative definition of $G^{(\ell+1)}(x)$ matches the placement of $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively in the definition of δ. This completes the induction.

The case $\ell = m - 1$ then shows that $F^{(m)}(x) = F(x)$ and $G^{(m)}(x) = G(x)$ form a complementary function pair, where $F^{(m)}(x)$ corresponds to the complete matrix M. Since $\delta'(i) = \delta(i) - (c_i - d_i^*) \cdot \mathbf{1}$, the placements of $A(x^{2^t})$ and $B(x^{2^t})$ in $G(x)$ correspond to the placements of $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively, in δ'. And since the iterative definition of $F(x)$ and $G(x)$ is based on the iterative construction of $(\boldsymbol{c}, \boldsymbol{d}^*)$, $G(x)$ corresponds to the complete matrix M'. ■

For example, consider once again the Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ in (5) and (6) respectively. The pair $(\boldsymbol{c}, \boldsymbol{d})$ can be obtained by taking $H = 4$, $m = 2$, $(\pi(1), \pi(2)) = (1, 2)$, $(e_1, e_2) = (0, 0)$, and $(e_0, e_0') = (0, 0)$ in (1). By Lemma 5 with $m = 2$ and $t = 1$, the sequences

$$\boldsymbol{f}'' = (0,0,1,1,2,2,1,1,0,2,1,3,0,2,3,1)$$
$$\boldsymbol{g}'' = (0,2,1,3,2,0,1,3,0,0,1,1,0,0,3,3)$$

obtained from the respective matrices

$$M = \begin{bmatrix} (\boldsymbol{a} + \mathbf{0}) & (\boldsymbol{b} + \mathbf{0}) \\ (\boldsymbol{a} + \mathbf{0}) & (\boldsymbol{b} + 2 \cdot \mathbf{1}) \end{bmatrix} = \begin{bmatrix} (0,1,2,1) & (0,1,0,3) \\ (0,1,2,1) & (2,3,2,1) \end{bmatrix}$$
$$M' = \begin{bmatrix} (\boldsymbol{a} + \mathbf{0}) & (\boldsymbol{b} + \mathbf{0}) \\ (\boldsymbol{a} + 2 \cdot \mathbf{1}) & (\boldsymbol{b} + \mathbf{0}) \end{bmatrix} = \begin{bmatrix} (0,1,2,1) & (0,1,0,3) \\ (2,3,0,3) & (0,1,0,3) \end{bmatrix}$$

form a quaternary Golay pair of length 16.

The intersections of Lemmas 3, 4 and 5 are shown in Figure 1. We claim that, given $e_0 = e_0'$ in (1), Lemma 5 becomes a special case of Lemma 3 when $t = 0$, and a special case of Lemma 4 when $t = m$. To establish this we need to show that, for a standard Golay pair $(\boldsymbol{c}, \boldsymbol{d})$ of length 2^m over $\mathbb{Z}_H$, the conditions controlling the choice of sequence elements in the three lemmas are equivalent, which follows from the equivalence of the following statements: $i_{\pi(1)} = 0$, $c_i = d_i$, and $d_i^* \ne c_i^*$. Given that $e_0 = e_0'$, from (1) we have

$$\boldsymbol{c} - \boldsymbol{d} = H/2 \cdot \boldsymbol{x}_{\pi(1)}. \tag{8}$$

Recall from Section II that $x_{\pi(1)}$ is the indicator function for $i_{\pi(1)}$ (which is bit $\pi(1)$ in the binary representation of i), so that $(\boldsymbol{x}_{\pi(1)})_i = i_{\pi(1)}$. Therefore (8) implies that $c_i - d_i = (H/2) i_{\pi(1)}$, and taking negative reversals of (8) likewise implies that $d_i^* - c_i^* = (H/2)(i_{\pi(1)} - 1)$. This gives the required equivalences.

D. *An interesting example*

As described in Section I, our principal objective is to count and to construct explicitly all quaternary Golay sequences and pairs of length 2^m obtained by applying Budišin's iterative construction to the non-standard Golay pairs of Theorem 2. We will achieve this using Lemma 5 and its variation Lemma 7 (to be introduced in Section IV-E). However we note here an interesting example obtained using Lemmas 3 and 5 that achieves another of our objectives, by constructing length 2^m quaternary Golay sequences and pairs that cannot be obtained by iterative application of Budišin's construction to a non-standard Golay pair specified in Theorem 2. This will demonstrate that Lemma 3 (and, by a similar example, Lemma 4) is not a special case of Lemma 5, even when its controlling pair is restricted to have length 2^m.

Example 6. *Let $\boldsymbol{a} = (a_0, a_1, \ldots, a_7)$ and $\boldsymbol{b} = (b_0, b_1, \ldots, b_7)$ be the non-standard length 8 quaternary Golay pair*

$$\begin{aligned} \boldsymbol{a} &= 2(x_1 x_2 + x_2 x_3) \\ &= (0,0,0,2,0,0,2,0) \\ \boldsymbol{b} &= 2(x_1 x_2 + x_1 x_3) + x_2 + x_3 \\ &= (0,1,1,2,0,3,3,2), \end{aligned}$$

specified in Theorem 2. Then the length 16 quaternary Golay pair

$$\boldsymbol{c} = \left[(\boldsymbol{a}+\mathbf{0}) \quad (\boldsymbol{b}+2\cdot\mathbf{1})\right]$$
$$\boldsymbol{d} = \left[(\boldsymbol{a}+\mathbf{0}) \quad (\boldsymbol{b}+\mathbf{0})\right],$$

obtained from Lemma 5 (or Lemma 3) using the seed pair $(\boldsymbol{a},\boldsymbol{b})$ and the controlling pair $((0,2),(0,0))$, is non-standard (and the algebraic normal form of each of $\boldsymbol{c}$ and $\boldsymbol{d}$ is a cubic polynomial [5]). Furthermore $\boldsymbol{c}-\boldsymbol{d} = \left[(\mathbf{0}) \quad (2\cdot\mathbf{1})\right]$ is the lifting of a binary sequence to $\mathbb{Z}_4$.

So we can apply Lemma 3 with controlling pair $(\boldsymbol{c},\boldsymbol{d})$ and seed pair $(\boldsymbol{a},\boldsymbol{b})$ to obtain a length $16\cdot 8 = 128$ quaternary Golay pair

$$\begin{aligned}\boldsymbol{f} &= [(\boldsymbol{a}+a_0\cdot\mathbf{1}) \quad \cdots \quad (\boldsymbol{a}+a_7\cdot\mathbf{1}) \\ &\qquad (\boldsymbol{b}+(b_0+2)\cdot\mathbf{1}) \quad \cdots \quad (\boldsymbol{b}+(b_7+2)\cdot\mathbf{1})] \\ \boldsymbol{g} &= [(\boldsymbol{a}-b_7\cdot\mathbf{1}) \quad \cdots \quad (\boldsymbol{a}-b_0\cdot\mathbf{1}) \\ &\qquad (\boldsymbol{b}-a_7\cdot\mathbf{1}) \quad \cdots \quad (\boldsymbol{b}-a_0\cdot\mathbf{1})],\end{aligned}$$

(and the algebraic normal form of each of $\boldsymbol{f}$ and $\boldsymbol{g}$ is a cubic polynomial,) and the elements of the sequence

$$\begin{aligned}\boldsymbol{f}-\boldsymbol{g} = \ &[((a_0+b_7)\cdot\mathbf{1}) \quad \cdots \quad ((a_7+b_0)\cdot\mathbf{1}) \\ &\qquad ((a_7+b_0+2)\cdot\mathbf{1}) \quad \cdots \quad ((a_0+b_7+2)\cdot\mathbf{1})]\end{aligned}$$

take all four values in $\mathbb{Z}_4$.

Now suppose, for a contradiction, that the Golay pair $(\boldsymbol{f},\boldsymbol{g})$ of Example 6 is the output of Lemma 5 for some seed pair $(\boldsymbol{a},\boldsymbol{b})$ and standard controlling pair $(\boldsymbol{c},\boldsymbol{d})$. In the notation of that lemma, all elements of $\boldsymbol{f}-\boldsymbol{g}$ must then belong to sequences $\delta(i)-\delta'(i) = (\boldsymbol{c}-\boldsymbol{d}^*)_i\cdot\mathbf{1}$ for varying i. Since $(\boldsymbol{c},\boldsymbol{d})$ is a standard Golay pair, the relations (2) show that

$$\boldsymbol{c}-\boldsymbol{d}^* = H/2\cdot\boldsymbol{x}_{\pi(m)} + e\cdot\mathbf{1} \quad \text{for some } e\in\mathbb{Z}_H. \tag{9}$$

Therefore the elements of $\boldsymbol{f}-\boldsymbol{g}$ take values only in $\{e, e+H/2\}$ for some $e\in\mathbb{Z}_H$. This contradicts the conclusion of Example 6.

Therefore the Golay pair $(\boldsymbol{f},\boldsymbol{g})$ of Example 6 is not just non-standard: it cannot be the output of Lemma 5, nor of Lemma 7 by a similar argument, nor of any other published construction for Golay sequences of which we are aware. (It is also easily verified by computer that there is no length 128 quaternary sequence $\boldsymbol{g}'$ forming a Golay pair with the sequence $\boldsymbol{f}$ of Example 6 such that $\boldsymbol{f}-\boldsymbol{g}'$ is a two-valued sequence.)

Example 6 can be generalized in several ways to give further examples of quaternary Golay pairs $(\boldsymbol{f},\boldsymbol{g})$ for which the elements of $\boldsymbol{f}-\boldsymbol{g}$ take more than two values. Lemma 4 can be used instead of Lemma 3. The seed pair $(\boldsymbol{a},\boldsymbol{b})$ used in the final application of Lemma 3 can be replaced by a different non-standard pair specified in Theorem 2, by the output of Theorem 10, or even by these further examples themselves. The controlling pair $(\boldsymbol{c},\boldsymbol{d})$ used in the final application of Lemma 3 can be of length $2^m\cdot 16$ for any $m\geq 0$, by applying Lemma 5 iteratively with controlling pair $((0,2),(0,0))$ and initial seed pair $(\boldsymbol{a},\boldsymbol{b})$. In this way we obtain quaternary Golay pairs of length $2^m\cdot 16\cdot 8 = 2^{m+7}$ for all $m\geq 0$, and these pairs cannot be produced using any other known constructions. Figure 2 illustrates these generalizations of Example 6.

E. Negative reversals

In this subsection we complete the framework of constructions by modifying Lemma 5 to use the negative reversals $\boldsymbol{a}^*$ and $\boldsymbol{b}^*$ of the seed pair sequences, as well as the sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ themselves. This allows the construction of Golay pairs that cannot be obtained with Lemma 5.

We then indicate by example that this modification corresponds to replacing some intermediate sequence in the iterative proof of Lemma 5 by its negative reversal. Since the aperiodic autocorrelation function of a sequence does not change under negative reversal, the remaining iterations of the construction still produce a Golay pair. This modification of Lemma 5, presented as Lemma 7, is not needed to produce the standard Golay pairs of length 2^m over $\mathbb{Z}_H$, but will be required to construct additional families of non-standard quaternary Golay pairs of length 2^m in Section V.

Lemma 7. *Let $(\boldsymbol{a},\boldsymbol{b})$ be a Golay pair of length n over $\mathbb{Z}_H$. Let $\boldsymbol{c}=(c_0,c_1,\ldots,c_{2^m-1})$ and $\boldsymbol{d}=(d_0,d_1,\ldots,d_{2^m-1})$ be a standard Golay pair of length 2^m over $\mathbb{Z}_H$, satisfying (1) for some permutation π of $\{1,\ldots,m\}$ and $e_0',e_0,e_1,\ldots,e_m\in\mathbb{Z}_H$. Write $(i_1,i_2,\ldots,i_m)$ for the binary representation of the integer i in the range $0\leq i<2^m$, and let ℓ be an integer in the range $2\leq\ell\leq m$. Define length n sequences*

$$\delta(i) := \begin{cases}\boldsymbol{a}+c_i\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=0 \text{ and } i_{\pi(\ell)}=0\\ \boldsymbol{b}+c_i\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=1 \text{ and } i_{\pi(\ell)}=0\\ \boldsymbol{b}^*+c_i\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=0 \text{ and } i_{\pi(\ell)}=1\\ \boldsymbol{a}^*+c_i\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=1 \text{ and } i_{\pi(\ell)}=1,\end{cases}$$

$$\delta'(i) := \begin{cases}\boldsymbol{a}+d_i^*\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=0 \text{ and } i_{\pi(\ell)}=0\\ \boldsymbol{b}+d_i^*\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=1 \text{ and } i_{\pi(\ell)}=0\\ \boldsymbol{b}^*+d_i^*\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=0 \text{ and } i_{\pi(\ell)}=1\\ \boldsymbol{a}^*+d_i^*\cdot\mathbf{1} & \text{if } i_{\pi(\ell-1)}=1 \text{ and } i_{\pi(\ell)}=1.\end{cases}$$

Then, for any integer t satisfying $0\leq t\leq m$, the sequence $\boldsymbol{f}$ obtained from the $2^t\times 2^{m-t}$ matrix

$$M := \begin{bmatrix}\delta(0) & \delta(2^t) & \cdots & \delta(2^m-2^t)\\ \delta(1) & \delta(2^t+1) & & \\ \vdots & & \ddots & \vdots\\ \delta(2^t-1) & \delta(2\cdot 2^t-1) & \cdots & \delta(2^m-1)\end{bmatrix}$$

forms a Golay pair of length $2^m n$ over $\mathbb{Z}_H$ with the sequence $\boldsymbol{g}$ obtained from the $2^t\times 2^{m-t}$ matrix

$$M' := \begin{bmatrix}\delta'(0) & \delta'(2^t) & \cdots & \delta'(2^m-2^t)\\ \delta'(1) & \delta'(2^t+1) & & \\ \vdots & & \ddots & \vdots\\ \delta'(2^t-1) & \delta'(2\cdot 2^t-1) & \cdots & \delta'(2^m-1)\end{bmatrix}.$$

Proof: The proof is similar to that of Lemma 5. ■

For example, take $H=4$, $m=4$, $(\pi(1),\pi(2),\pi(3),\pi(4)) = (4,3,1,2)$, $(e_1,e_2,e_3,e_4) = (0,0,2,1)$, and $(e_0,e_0') = (0,1)$ in (1) to give the standard length 16 quaternary Golay pair

$$\boldsymbol{c} = (0,1,2,1,0,1,2,1,0,1,0,3,2,3,2,1)$$
$$\boldsymbol{d} = (1,0,3,0,1,0,3,0,1,0,1,2,3,2,3,0),$$

and use this standard pair in Lemma 7 with $\ell = 3$ and $t = 2$ to obtain the sequences $\boldsymbol{f}$, $\boldsymbol{g}$ of a Golay pair from the respective matrices

$$M = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{b}^*+\mathbf{0}) & (\boldsymbol{b}^*+2\cdot\mathbf{1}) \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{b}^*+1\cdot\mathbf{1}) & (\boldsymbol{b}^*+3\cdot\mathbf{1}) \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{a}^*+\mathbf{0}) & (\boldsymbol{a}^*+2\cdot\mathbf{1}) \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{a}^*+3\cdot\mathbf{1}) & (\boldsymbol{a}^*+1\cdot\mathbf{1}) \end{bmatrix}$$

$$M' = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & (\boldsymbol{a}+2\cdot\mathbf{1}) & (\boldsymbol{b}^*+\mathbf{0}) & (\boldsymbol{b}^*+\mathbf{0}) \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & (\boldsymbol{a}+3\cdot\mathbf{1}) & (\boldsymbol{b}^*+1\cdot\mathbf{1}) & (\boldsymbol{b}^*+1\cdot\mathbf{1}) \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & (\boldsymbol{b}+\mathbf{0}) & (\boldsymbol{a}^*+\mathbf{0}) & (\boldsymbol{a}^*+\mathbf{0}) \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & (\boldsymbol{b}+3\cdot\mathbf{1}) & (\boldsymbol{a}^*+3\cdot\mathbf{1}) & (\boldsymbol{a}^*+3\cdot\mathbf{1}) \end{bmatrix}.$$

We now show that the same Golay pair $(\boldsymbol{f}, \boldsymbol{g})$ can alternatively be obtained from the iterative construction given in the proof of Lemma 5 (using a different permutation $\tilde{\pi}$), by replacing the intermediate sequence corresponding to the matrix $M'^{(2)}$ in that construction by its negative reversal. Take $H = 4$, $m = 4$, and $t = 2$ again, and let $(\tilde{\pi}(1), \tilde{\pi}(2), \tilde{\pi}(3), \tilde{\pi}(4)) = (3, 4, 1, 2)$, $(\tilde{e_1}, \tilde{e_2}, \tilde{e_3}, \tilde{e_4}) = (3, 0, 2, 1)$, and $(\tilde{e_0}, \tilde{e_0}') = (0, 2)$. This produces the standard length 16 quaternary Golay pair $(\boldsymbol{c}, \boldsymbol{d})$ previously given as an example in Section IV-B and, as seen in Section IV-C, steps 1 and 2 of the iterative construction lead to the intermediate matrices

$$M^{(2)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \end{bmatrix}$$

$$M'^{(2)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}+3\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}+3\cdot\mathbf{1}) & \cdot & \cdot & \cdot \end{bmatrix}.$$

We now replace the sequence corresponding to $M'^{(2)}$ by its negative reversal, so that $M'^{(2)}$ is replaced by

$$\begin{bmatrix} (\boldsymbol{b}^*+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{b}^*+2\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}^*+1\cdot\mathbf{1}) & \cdot & \cdot & \cdot \\ (\boldsymbol{a}^*+\mathbf{0}) & \cdot & \cdot & \cdot \end{bmatrix}.$$

Proceeding with the iterative construction, we now find at step 3 that

$$M^{(3)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & (\boldsymbol{b}^*+\mathbf{0}) & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}^*+1\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}^*+\mathbf{0}) & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}^*+3\cdot\mathbf{1}) & \cdot \end{bmatrix}$$

$$M'^{(3)} = \begin{bmatrix} (\boldsymbol{a}+\mathbf{0}) & \cdot & (\boldsymbol{b}^*+2\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{a}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{b}^*+3\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+2\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}^*+2\cdot\mathbf{1}) & \cdot \\ (\boldsymbol{b}+1\cdot\mathbf{1}) & \cdot & (\boldsymbol{a}^*+1\cdot\mathbf{1}) & \cdot \end{bmatrix},$$

and at step 4 we obtain $M^{(4)} = M$ and $M'^{(4)} = M'$ as claimed.

For given H, m and t, suppose the permutation π and constants $e_0, e_1, \ldots, e_m$ are used in Lemma 7 with the value ℓ. Define the permutation σ by

$$\sigma = (1, \ell-1)(2, \ell-2)\cdots(\lfloor(\ell-1)/2\rfloor, \lceil(\ell+1)/2\rceil).$$

Then we can show that in general the resulting Golay pair $(\boldsymbol{f}, \boldsymbol{g})$ can also be obtained from Lemma 5 using the permutation $\tilde{\pi}(i) := \pi(\sigma(i))$ and constants $\tilde{e_0}, \tilde{e_1}, \ldots, \tilde{e_m}$, where

$$\begin{aligned} \tilde{e}_{\tilde{\pi}(i)} &= e_{\tilde{\pi}(i)} \quad \text{for } i \neq \ell \\ \tilde{e}_{\tilde{\pi}(\ell)} &= c_{\sum_{i=1}^{\ell} 2^{m-\pi(i)}} - c_{2^{m-\pi(\ell)}} \\ \tilde{e}_0 &= e_0, \end{aligned}$$

by replacing the sequence $G^{(\ell-1)}(x)$ corresponding to $M'^{(\ell-1)}$ by its negative reversal prior to step ℓ (in which $F^{(\ell)}(x)$ and $G^{(\ell)}(x)$ are determined). We can also show that at most one negative reversal is sufficient for construction purposes: introducing further negative reversals of intermediate sequences in the iterative construction does not lead to any more Golay pairs. These two statements imply that Lemma 7 encapsulates the effect of taking arbitrary negative reversals of intermediate sequences in the iterative construction described in the proof of Lemma 5. We omit the proofs as they are rather involved, and are not required in the construction of families of Golay sequences and pairs in Section V.

For a fixed value of m, the sequences obtained from Lemma 5 are identical to those obtained from Lemma 7 in some cases (for example when $(\boldsymbol{a}, \boldsymbol{b})$ varies over all standard pairs of a given length and $(\boldsymbol{c}, \boldsymbol{d})$ varies over all standard pairs of length 2^m), but are disjoint in others (for example the sequences constructed in Theorem 10, which arise from certain non-standard pairs $(\boldsymbol{a}, \boldsymbol{b})$).

V. Spawned sequences and pairs

In this section we determine explicitly the algebraic normal form of the Golay sequences and pairs of length 2^{m+r} ($m \geq 1$) that are spawned by an arbitrary seed pair $(\boldsymbol{a}, \boldsymbol{b})$ of length 2^r under either of Lemmas 5 and 7. We then apply this result to the non-standard quaternary Golay pairs given in Theorem 2.

Throughout this section we take the seed pair $(\boldsymbol{a}, \boldsymbol{b})$ to have length 2^r. We begin by determining the algebraic normal form of the Golay pairs $(\boldsymbol{f}, \boldsymbol{g})$ that can be constructed from the case $t = 0$ of Lemma 5 or 7.

Lemma 8. *Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Golay pair of length 2^r over $\mathbb{Z}_H$ and let $\boldsymbol{c}$ be a standard Golay sequence of length 2^m over $\mathbb{Z}_H$ satisfying (1) for some permutation π of $\{1, 2, \ldots, m\}$. Let $a(x_1, x_2, \ldots, x_r)$, $b(x_1, x_2, \ldots, x_r)$, $c(x_1, x_2, \ldots, x_m)$ be the algebraic normal form of $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ respectively, and let ℓ be an integer in the range $2 \leq \ell \leq m$. Then, for any $e \in \mathbb{Z}_H$, the sequence pair*

$$\begin{cases} f(x_1, x_2, \ldots, x_{m+r}) \\ f(x_1, x_2, \ldots, x_{m+r}) + \dfrac{H}{2} x_{\pi(m)} + e \end{cases}$$

is a Golay pair of length 2^{m+r} over $\mathbb{Z}_H$, where

$$\begin{aligned} f(x_1, x_2, \ldots, x_{m+r}) &:= \\ &\quad a(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot (1 - x_{\pi(1)}) \\ &+ b(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot x_{\pi(1)} \\ &+ c(x_1, x_2, \ldots, x_m) \end{aligned}$$

is produced by the case $t = 0$ of Lemma 5, or alternatively

$$\begin{aligned} f(x_1, x_2, \ldots, x_{m+r}) &:= \\ &a(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot (1 - x_{\pi(\ell-1)}) \cdot (1 - x_{\pi(\ell)}) \\ &+ b(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot x_{\pi(\ell-1)} \cdot (1 - x_{\pi(\ell)}) \\ &+ b^*(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot (1 - x_{\pi(\ell-1)}) \cdot x_{\pi(\ell)} \\ &+ a^*(x_{m+1}, x_{m+2}, \ldots, x_{m+r}) \cdot x_{\pi(\ell-1)} \cdot x_{\pi(\ell)} \\ &+ c(x_1, x_2, \ldots, x_m) \end{aligned}$$

is produced by the case $t = 0$ of Lemma 7.

Proof: We give the proof for the case $t = 0$ of Lemma 5; the proof for Lemma 7 is similar. For any $e_0' \in \mathbb{Z}_H$, the sequence $\boldsymbol{c}$ forms a standard Golay pair with a sequence $\boldsymbol{d}$ satisfying (1). By (9), we can choose e_0' so that the algebraic normal form of $\boldsymbol{d}^*$ is given by $d^*(x_1, x_2, \ldots, x_m) = c(x_1, x_2, \ldots, x_m) + (H/2)x_{\pi(m)} + e$. We then apply the case $t = 0$ of Lemma 5, using $(\boldsymbol{a}, \boldsymbol{b})$ as the seed pair and $(\boldsymbol{c}, \boldsymbol{d})$ as the controlling pair, to produce the Golay pair $(\boldsymbol{f}, \boldsymbol{g})$.

Let $(i_1, i_2, \ldots, i_m)$ be the binary representation of the integer i in the range $0 \le i < 2^m$. The sequence $\boldsymbol{f}$ is formed by placing a copy of $\boldsymbol{a}$ whenever $i_{\pi(1)} = 0$ and a copy of $\boldsymbol{b}$ whenever $i_{\pi(1)} = 1$, and then adding the sequence $(c_0 \cdot \mathbf{1}, c_1 \cdot \mathbf{1}, \ldots, c_{2^m-1} \cdot \mathbf{1})$. Since x_j is the indicator function for i_j, this gives the claimed algebraic normal form $f(x_1, x_2, \ldots, x_{m+r})$ of $\boldsymbol{f}$.

The same analysis holds for $\boldsymbol{g}$, except that the sequence $(d_0^* \cdot \mathbf{1}, d_1^* \cdot \mathbf{1}, \ldots, d_{2^m-1}^* \cdot \mathbf{1})$ is added instead of $(c_0 \cdot \mathbf{1}, c_1 \cdot \mathbf{1}, \ldots, c_{2^m-1} \cdot \mathbf{1})$. ■

We next relate the algebraic normal form of the Golay pairs $(\boldsymbol{f}, \boldsymbol{g})$ that can be constructed from Lemma 5 or 7 for general t (satisfying $0 \le t \le m$) to the form for the case $t = 0$ determined in Lemma 8.

Lemma 9. *Let $(f(x_1, x_2, \ldots, x_{m+r}),\ g(x_1, x_2, \ldots, x_{m+r}))$ be a Golay pair of length 2^{m+r} produced by the case $t = 0$ of Lemma 5 or 7, using a seed pair $(\boldsymbol{a}, \boldsymbol{b})$ of length 2^r over $\mathbb{Z}_H$ and a controlling pair $(\boldsymbol{c}, \boldsymbol{d})$ of length 2^m over $\mathbb{Z}_H$ satisfying (1). Let $(\boldsymbol{f}', \boldsymbol{g}')$ be the Golay pair produced under the same conditions, but for general t satisfying $0 \le t \le m$. Then the algebraic normal form of $\boldsymbol{f}'$, $\boldsymbol{g}'$ is respectively*

$$\begin{aligned} &f(x_{\phi(1)}, x_{\phi(2)}, \ldots, x_{\phi(m+r)}), \\ &g(x_{\phi(1)}, x_{\phi(2)}, \ldots, x_{\phi(m+r)}), \end{aligned}$$

where ϕ is the permutation of $\{1, 2, \ldots, m+r\}$ given by

$$\phi(i) = \begin{cases} i & \text{if } 1 \le i \le m - t \\ i + r & \text{if } m - t + 1 \le i \le m \\ i - t & \text{if } m + 1 \le i \le m + r. \end{cases} \tag{10}$$

Proof: We give the proof for $\boldsymbol{f}'$; the proof for $\boldsymbol{g}'$ is very similar. There is nothing to prove for $t = 0$ so fix $t > 0$, and fix integers k, ℓ, p satisfying $0 \le k < 2^t$, $0 \le \ell < 2^{m-t}$, $0 \le p < 2^r$.

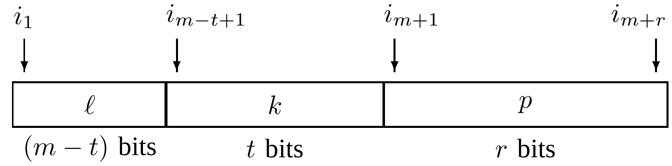
Let $M_{\boldsymbol{f}}$ be the 1×2^m matrix corresponding to $\boldsymbol{f}$ and let $M_{\boldsymbol{f}'}$ be the $2^t \times 2^{m-t}$ matrix corresponding to $\boldsymbol{f}'$, as in Lemma 5 or 7. The sequences $\boldsymbol{f}$ and $\boldsymbol{f}'$ are obtained by reading the entries of these matrices column by column, and so the sequence $\delta(2^t\ell + k)$ occurs in row 0 and column $2^t\ell + k$ of $M_{\boldsymbol{f}}$, and in row k and column ℓ of $M_{\boldsymbol{f}'}$. Since each sequence $\delta(i)$ has length 2^r, it follows that entry p of the sequence $\delta(2^t\ell + k)$ occurs in

$$\text{position } i := (2^t\ell + k)2^r + p \quad \text{of } \boldsymbol{f} \tag{11}$$

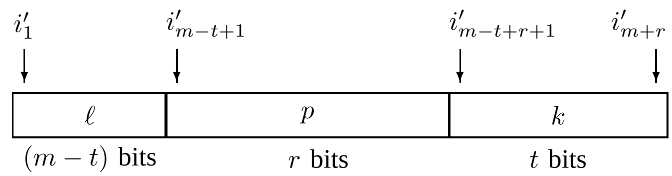
and in

$$\text{position } i' := (2^t\ell)2^r + (2^t)p + k \quad \text{of } \boldsymbol{f}'. \tag{12}$$

Let $(i_1, i_2, \ldots, i_{m+r})$ be the binary representation of $i = \sum_{j=1}^{m+r} 2^{m+r-j} i_j$, which by (11) we can depict in block form as:



Similarly, by (12) we can depict the binary representation of i' as:



in which the two rightmost blocks of bits of i have been interchanged.

Since x_j is the indicator function for i_j and i'_j, and $f(x_1, x_2, \ldots, x_{m+r})$ is the algebraic normal form of $\boldsymbol{f}$, it follows that the algebraic normal form of $\boldsymbol{f}'$ is

$$f(x_{\phi(1)}, x_{\phi(2)}, \ldots, x_{\phi(m+r)})$$

(so, for example, each occurrence of bit $m - t + 1$ in i is replaced by bit $m - t + r + 1$ in i'). ■

For example, consider again the constructed Golay pairs $(\boldsymbol{f}, \boldsymbol{g})$, $(\boldsymbol{f}', \boldsymbol{g}')$, and $(\boldsymbol{f}'', \boldsymbol{g}'')$ given directly after the proof of Lemmas 3, 4 and 5 respectively, all of which can be obtained from Lemma 5 with $m = r = 2$ and with $t = 0$, $t = 1$, and $t = 2$ respectively. The case $t = 0$ is given by

$$\boldsymbol{f} = (0, 1, 2, 1, 0, 1, 2, 1, 0, 1, 0, 3, 2, 3, 2, 1),$$

so that

$$f(x_1, x_2, x_3, x_4) = 2(x_1x_2 + x_1x_3 + x_3x_4) + 2x_3 + x_4.$$

The case $t = 1$ is given by

$$\begin{aligned} \boldsymbol{f}'' &= (0, 0, 1, 1, 2, 2, 1, 1, 0, 2, 1, 3, 0, 2, 3, 1) \\ &= 2(x_1x_4 + x_1x_2 + x_2x_3) + 2x_2 + x_3 \\ &= f(x_1, x_4, x_2, x_3), \end{aligned}$$

and the case $t = 2$ is given by

$$\begin{aligned} \boldsymbol{f}' &= (0, 0, 0, 2, 1, 1, 1, 3, 2, 2, 0, 2, 1, 1, 3, 1) \\ &= 2(x_3x_4 + x_3x_1 + x_1x_2) + 2x_1 + x_2 \\ &= f(x_3, x_4, x_1, x_2), \end{aligned}$$

in accordance with Lemma 9. Similarly we have $g(x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4) + 2x_2$ and $\boldsymbol{g}'' = g(x_1, x_4, x_2, x_3)$, $\boldsymbol{g}' = g(x_3, x_4, x_1, x_2)$.

We have now assembled all the ingredients needed to achieve our principal objective, namely to determine explicitly the quaternary Golay sequences and pairs of length 2^{m+3} ($m \geq 1$) obtained by applying Lemmas 5 and 7 to the 512 non-standard quaternary ordered Golay seed pairs $(\boldsymbol{a}, \boldsymbol{b})$ of length 8 described in Theorem 2.

Theorem 10. *Let $m \geq 1$ be an integer, and let t and ℓ be integers in the range $0 \leq t \leq m$ and $2 \leq \ell \leq m$. Let τ be a bijection between $\{1, \ldots, m\}$ and $\{1, \ldots, m+3\} \setminus \{m-t+1, m-t+2, m-t+3\}$. Then, for any $e, e_0, e_1, \ldots, e_m \in \mathbb{Z}_4$ and $u_0, u_1, u_2, u_3 \in \mathbb{Z}_2$, the sequence pair*

$$\begin{cases} f(x_1, x_2, \ldots, x_{m+3}) \\ f(x_1, x_2, \ldots, x_{m+3}) + 2x_{\tau(m)} + e \end{cases}$$

is a non-standard quaternary Golay pair of length 2^{m+3}, where $f(x_1, x_2, \ldots, x_{m+3})$ takes any one of the four forms:

$$\begin{aligned} &f_1(x_1, x_2, \ldots, x_{m+3}) + 2x_{m-t+2}x_{m-t+3} \\ &+ 2u_0x_{m-t+1} + 2u_3x_{m-t+2} + (2u_0 + 2u_2 + u_3)x_{m-t+3}; \end{aligned} \tag{13}$$

$$\begin{aligned} &f_1(x_1, x_2, \ldots, x_{m+3}) + 2x_{m-t+1}x_{m-t+3} + 2x_{m-t+2}x_{\tau(1)} \\ &+ 2x_{m-t+3}x_{\tau(1)} + (2u_1 + 2u_2 + 2u_3 + 1)x_{m-t+2} \\ &+ (2u_1 + u_3 + 1)x_{m-t+3}; \end{aligned} \tag{14}$$

$$\begin{aligned} &f_2(x_1, x_2, \ldots, x_{m+3}) + 2x_{m-t+2}x_{m-t+3} \\ &+ 2u_0x_{m-t+1} + 2u_3x_{m-t+2} + (2u_0 + 2u_2 + u_3)x_{m-t+3}; \end{aligned} \tag{15}$$

$$\begin{aligned} &f_2(x_1, x_2, \ldots, x_{m+3}) + 2x_{m-t+1}x_{m-t+3} + 2x_{m-t+2}x_{\tau(\ell-1)} \\ &+ 2x_{m-t+3}x_{\tau(\ell-1)} + 2x_{m-t+1}x_{\tau(\ell)} + 2x_{m-t+3}x_{\tau(\ell)} \\ &+ (2u_1 + 2u_2 + 2u_3 + 1)x_{m-t+2} + (2u_1 + u_3 + 1)x_{m-t+3}, \end{aligned} \tag{16}$$

where

$$\begin{aligned} &f_1(x_1, x_2, \ldots, x_{m+3}) := \\ &\quad 2x_{m-t+1}x_{m-t+3}x_{\tau(1)} + 2x_{m-t+2}x_{m-t+3}x_{\tau(1)} \\ &+ 2x_{m-t+1}x_{m-t+2} + 2u_0x_{m-t+1}x_{\tau(1)} \\ &+ (2u_1 + 2u_2 + 1)x_{m-t+2}x_{\tau(1)} \\ &+ (2u_0 + 2u_1 + 2u_2 + 1)x_{m-t+3}x_{\tau(1)} \\ &+ 2\sum_{k=1}^{m-1} x_{\tau(k)}x_{\tau(k+1)} + \sum_{k=1}^{m} e_kx_{\tau(k)} + e_0 \end{aligned}$$

and

$$\begin{aligned} &f_2(x_1, x_2, \ldots, x_{m+3}) := \\ &\quad 2x_{m-t+1}x_{m-t+3}x_{\tau(\ell-1)} + 2x_{m-t+2}x_{m-t+3}x_{\tau(\ell-1)} \\ &+ 2x_{m-t+1}x_{m-t+3}x_{\tau(\ell)} + 2x_{m-t+2}x_{m-t+3}x_{\tau(\ell)} \\ &+ 2x_{m-t+1}x_{\tau(\ell-1)}x_{\tau(\ell)} + 2x_{m-t+3}x_{\tau(\ell-1)}x_{\tau(\ell)} \\ &+ 2x_{m-t+1}x_{m-t+2} + 2u_0x_{m-t+1}x_{\tau(\ell-1)} \\ &+ (2u_1 + 2u_2 + 1)x_{m-t+2}x_{\tau(\ell-1)} \\ &+ (2u_0 + 2u_1 + 2u_2 + 1)x_{m-t+3}x_{\tau(\ell-1)} \\ &+ 2u_0x_{m-t+1}x_{\tau(\ell)} + (2u_1 + 2u_2 + 3)x_{m-t+2}x_{\tau(\ell)} \\ &+ (2u_0 + 2u_1 + 2u_2 + 3)x_{m-t+3}x_{\tau(\ell)} \\ &+ 2\sum_{\substack{k=1 \\ k \neq \ell-1}}^{m-1} x_{\tau(k)}x_{\tau(k+1)} + \sum_{k=1}^{m} e_kx_{\tau(k)} + e_0. \end{aligned}$$

Proof: Fix $e, e_0, e_1, \ldots, e_m \in \mathbb{Z}_4$ and $u_0, u_1, u_2, u_3 \in \mathbb{Z}_2$. Let $(\boldsymbol{a}, \boldsymbol{b})$ be the non-standard quaternary Golay pair of length 8 given by

$$\left.\begin{aligned} a(x_1, x_2, x_3) = \;& 2x_1x_2 + 2x_2x_3 + 2u_0x_1 + 2u_3x_2 \\ & + (2u_0 + 2u_2 + u_3)x_3, \\ b(x_1, x_2, x_3) = \;& 2x_1x_2 + 2x_1x_3 \\ & + (2u_1 + 2u_2 + 2u_3 + 1)x_2 \\ & + (2u_1 + u_3 + 1)x_3 \end{aligned}\right\} \tag{17}$$

respectively, which is the case $k_0 = k_1 = 0$ of Theorem 2. Define the mapping $\pi(i) := \phi^{-1}(\tau(i))$, where ϕ is the permutation of $\{1, 2, \ldots, m+3\}$ given by the case $r = 3$ of (10). This mapping π is a permutation of $\{1, 2, \ldots, m\}$, so by (1) there is a standard Golay pair $(\boldsymbol{c}, \boldsymbol{d})$ for which $\boldsymbol{c}$ has the form

$$c(x_1, x_2, \ldots, x_m) = 2\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} e_kx_{\pi(k)} + e_0 \tag{18}$$

(setting e_k in (1) to be the fixed value $e_{\pi^{-1}(k)}$ for $1 \leq k \leq m$). The form (13) for $f(x_1, x_2, \ldots, x_{m+3})$ arises from application of Lemma 5 with seed pair $(\boldsymbol{a}, \boldsymbol{b})$; the form (14) from Lemma 5 with seed pair $(\boldsymbol{b}, \boldsymbol{a})$; the form (15) from Lemma 7 with seed pair $(\boldsymbol{a}, \boldsymbol{b})$; and the form (16) from Lemma 7 with seed pair $(\boldsymbol{b}, \boldsymbol{a})$. In all four cases the controlling pair used is $(\boldsymbol{c}, \boldsymbol{d})$. We give the proof for the form (13) in detail; the proof for the form (14) is very similar.

We wish to construct a quaternary Golay pair $(\boldsymbol{f}, \boldsymbol{g})$ of length 2^{m+3} from Lemma 5, using seed pair $(\boldsymbol{a}, \boldsymbol{b})$ and controlling pair $(\boldsymbol{c}, \boldsymbol{d})$. When $t = 0$, by Lemma 8 this pair $(\boldsymbol{f}, \boldsymbol{g})$ is given by

$$\begin{aligned} &f'(x_1, x_2, \ldots, x_{m+3}) := \\ &\quad a(x_{m+1}, x_{m+2}, x_{m+3}) \cdot (1 - x_{\pi(1)}) \\ &\quad + b(x_{m+1}, x_{m+2}, x_{m+3}) \cdot x_{\pi(1)} \\ &\quad + c(x_1, x_2, \ldots, x_m), \\ &g'(x_1, x_2, \ldots, x_{m+3}) := \\ &\quad f'(x_1, x_2, \ldots, x_{m+3}) + 2x_{\pi(m)} + e \end{aligned}$$

respectively. Therefore, for general t in the range $0 \leq t \leq m$, by Lemma 9 the pair $(\boldsymbol{f}, \boldsymbol{g})$ is given by

$$\begin{aligned}
&f'(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m+3)}) = \\
&\qquad a(x_{m-t+1}, x_{m-t+2}, x_{m-t+3}) \cdot (1 - x_{\phi(\pi(1))}) \\
&\qquad + b(x_{m-t+1}, x_{m-t+2}, x_{m-t+3}) \cdot x_{\phi(\pi(1))} \\
&\qquad + c(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m)}), \\
&g'(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m+3)}) = \\
&\qquad f'(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m+3)}) + 2x_{\phi(\pi(m))} + e.
\end{aligned}$$

Set $f(x_1, x_2, \dots, x_{m+3}) := f'(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m+3)})$ and $g(x_1, x_2, \dots, x_{m+3}) := g'(x_{\phi(1)}, x_{\phi(2)}, \dots, x_{\phi(m+3)})$. Substitute from (17) and (18), and use the definition of π, to show that

$$\begin{aligned}
&f(x_1, x_2, \dots, x_{m+3}) = \\
&\qquad [2x_{m-t+1}x_{m-t+2} + 2x_{m-t+2}x_{m-t+3} \\
&\qquad + 2u_0 x_{m-t+1} + 2u_3 x_{m-t+2} \\
&\qquad + (2u_0 + 2u_2 + u_3)x_{m-t+3}] \cdot (1 - x_{\tau(1)}) \\
&\qquad + [2x_{m-t+1}x_{m-t+2} + 2x_{m-t+1}x_{m-t+3} \\
&\qquad + (2u_1 + 2u_2 + 2u_3 + 1)x_{m-t+2} \\
&\qquad + (2u_1 + u_3 + 1)x_{m-t+3}] \cdot x_{\tau(1)} \\
&\qquad + 2\sum_{k=1}^{m-1} x_{\tau(k)}x_{\tau(k+1)} + \sum_{k=1}^{m} e_k x_{\tau(k)} + e_0, \\
&g(x_1, x_2, \dots, x_{m+3}) = \\
&\qquad f(x_1, x_2, \dots, x_{m+3}) + 2x_{\tau(m)} + e.
\end{aligned}$$

The claimed form (13) for the constructed sequence pair $(\boldsymbol{f}, \boldsymbol{g})$ is given by collecting terms. The algebraic normal forms contain cubic terms and so both constructed sequences are non-standard.

The proof for the forms (15) and (16) is similar, noting from (2) that

$$a^*(x_1, x_2, x_3) = a(x_1, x_2, x_3) + 2x_1 + 2x_3 + 2u_2 + u_3,$$

$$b^*(x_1, x_2, x_3) = b(x_1, x_2, x_3) + 2x_2 + 2x_3 + 2u_2 + u_3 + 2.$$

(The calculated forms for (15) and (16) initially contain terms $(2u_2 + u_3 + 2)x_{\tau(\ell)}$ and $(2u_2 + u_3)x_{\tau(\ell)}$ respectively but these terms have been absorbed into the linear sum $\sum_{k=1}^{m} e_k x_{\tau(k)}$, which corresponds in each case to an adjustment of the constant e_ℓ.) ∎

The quaternary Golay sequences and pairs constructed in Theorem 10 use the seed pair $(\boldsymbol{a}, \boldsymbol{b})$ given by the case $(k_0, k_1) = (0, 0)$ of Theorem 2, as stated in (17). We do not obtain further quaternary Golay sequences or pairs by using the seed pair given by any case $(k_0, k_1) \neq (0, 0)$ of Theorem 2. For example, application of Lemma 5 to the resulting seed pair $(\boldsymbol{a} + k_0 \cdot \mathbf{1}, \boldsymbol{b} + k_1 \cdot \mathbf{1})$ instead of to $(\boldsymbol{a}, \boldsymbol{b})$ replaces the constructed pair $(\boldsymbol{f}, \boldsymbol{f} + 2\boldsymbol{x}_{\tau(m)} + e \cdot \mathbf{1})$ by the pair $(\boldsymbol{f}', \boldsymbol{f}' + 2\boldsymbol{x}_{\tau(m)} + e \cdot \mathbf{1})$ where $\boldsymbol{f}' := \boldsymbol{f} + (k_1 - k_0)\boldsymbol{x}_{\tau(1)} + k_0 \cdot \mathbf{1}$, but this pair is already included in the first form of Theorem 10.

We now count the number of quaternary sequences and pairs constructed in Theorem 10.

Corollary 11. *For each integer $m \geq 1$ there are at least $(m+1)!(m+1) \cdot 4^{m+1} \cdot 16$ non-standard quaternary Golay sequences of length 2^{m+3} and at least $2(m+1)!(m+1) \cdot 4^{m+2} \cdot 16$ non-standard quaternary ordered Golay pairs of length 2^{m+3}.*

Proof: Each form (13), (14), (15), (16) gives rise to a set of sequences as the parameters t, ℓ, τ, $e_0, e_1, \dots, e_m$, u_0, u_1, u_2, u_3 vary over their ranges. By comparison of cubic terms, all sequences in the sets arising from (13) and (14) are distinct from those in the sets arising from (15) and (16). By comparison of quadratic terms, all sequences in the set arising from (13) are distinct from those arising from (14), and those arising from (15) are distinct from those arising from (16).

We firstly count the sequences in the sets arising from (13) and (14). There are $m!$ choices for τ; $m+1$ choices for t; 4^{m+1} choices for $e_0, e_1, \dots, e_m$; and 2^4 choices for u_0, u_1, u_2, u_3. Since τ is a bijection between $\{1, \dots, m\}$ and $\{1, \dots, m+3\} \setminus \{m-t+1, m-t+2, m-t+3\}$, each choice of parameters yields a distinct sequence (for example, we can consider $\{u_0, 2u_1 + 2u_2 + 1, u_3, 2u_0 + 2u_2 + u_3\}$ and $\{u_0, 2u_1 + 2u_2 + 3, 2u_1 + 2u_2 + 2u_3 + 1, 2u_1 + u_3 + 1\}$ to form a linearly independent set when considering (13) and (14) respectively). We therefore obtain exactly $m!(m+1) \cdot 4^{m+1} \cdot 2^4 \cdot 2$ distinct sequences from (13) and (14). No further sequences are obtained by considering the sequence $f(x_1, x_2, \dots, x_{m+3}) + 2x_{\tau(m)} + e$ that forms a Golay pair with the sequence $f(x_1, x_2, \dots, x_{m+3})$.

We next count the sequences in the sets arising from (15) and (16). Each sequence in the set arising from (15) is counted exactly twice as the parameters vary: the mapping $\ell \mapsto m + 2 - \ell$; $u_1 \mapsto u_1 + 1$; $\tau \mapsto \tau'$, where $\tau'(i) := \tau(m + 1 - i)$, leaves $\sum_{k=1}^{m-1} x_{\tau(k)}x_{\tau(k+1)}$ invariant but interchanges $\tau(\ell - 1)$ and $\tau(\ell)$, and interchanges $2u_1 + 1$ and $2u_1 + 3$. Similarly each sequence in the set arising from (16) is counted exactly twice, by considering the mapping $\ell \mapsto m + 2 - \ell$; $u_0 \mapsto u_0 + 1$; $\tau \mapsto \tau'$. Since there are $m - 1$ choices for ℓ, we therefore obtain exactly $m!(m+1)(m-1) \cdot 4^{m+1} \cdot 2^4 \cdot 2/2$ distinct sequences from (15) and (16), and no further sequences by considering $f(x_1, x_2, \dots, x_{m+3}) + 2x_{\tau(m)} + e$.

Summing the two counts gives the stated minimum number of non-standard quaternary Golay sequences of length 2^{m+3}.

We finally count the minimum number of Golay pairs formed from these sequences. Inspection of the algebraic normal forms shows, for each constructed sequence $\boldsymbol{f}$, that $\boldsymbol{f}^* \neq \boldsymbol{f} + c \cdot \mathbf{1}$ for any $c \in \mathbb{Z}_4$. Therefore we can partition the constructed sequences into sets of the form $E(\boldsymbol{f}) \cup E(\boldsymbol{g})$, each such set involving $2 \cdot 8 = 16$ sequences, such that $E(\boldsymbol{f}) \times E(\boldsymbol{g})$ comprises $8^2 \cdot 2 = 128$ ordered Golay pairs (see Section II). The minimum number of Golay pairs formed from the constructed sequences is therefore given by multiplying the sequence count by 8 (and the true number will exceed this minimum if two constructed sequences at smaller lengths have the shared autocorrelation property). ∎

Table I lists the known number of standard and non-standard length 2^m quaternary Golay sequences and pairs, using the counts from Corollary 11. The minimum values given for $m \geq 7$ are both strict minima, because of the generalization of Example 6 described at the end of Section IV. The values given for $m \leq 4$ are exact counts, by exhaustive computer search. But we do not currently know whether the minimum

	# quaternary Golay sequences		# quaternary ordered Golay pairs	
Length	standard	non-standard	standard	non-standard
4	64	0	512	0
8	768	0	6,144	512
16	12,288	1,024	98,304	8,192
32	245,760	$\geq$ 18,432	1,966,080	$\geq$ 147,456
64	5,898,240	$\geq$ 393,216	47,185,920	$\geq$ 3,145,728
2^m $(m \geq 7)$	$m!/2 \cdot 4^{m+1}$	$> (m-2)!(m-2) \cdot 4^m$	$m! \cdot 4^{m+2}$	$> 2(m-2)!(m-2) \cdot 4^{m+1}$

TABLE I
NUMBER OF LENGTH 2^m QUATERNARY GOLAY SEQUENCES AND ORDERED GOLAY PAIRS

values given for lengths 32 and 64 are exact counts. While we know that no two standard quaternary Golay sequences of length 32 have the shared autocorrelation property [5], it is possible that one of the non-standard quaternary Golay sequences of length 32 constructed in Theorem 10 has the shared autocorrelation property with a standard quaternary Golay sequence or with another non-standard quaternary Golay sequence constructed in Theorem 10. In that case we could construct further non-standard quaternary Golay sequences and pairs of length 64 and higher via the resulting cross-over of autocorrelation functions (see Figure 3). It is also possible that there are non-standard quaternary Golay sequences of length 32 or 64 that are not contained in Theorem 10.

For $h > 2$, the non-standard Golay sequences and pairs constructed in Theorem 10 and Example 6 (and its generalizations) give non-standard Golay sequences and pairs over $\mathbb{Z}_{2^h}$ under lifting and linear transformation (see the end of Section II).

VI. Conclusion

In this section we summarize the main results of the paper, clarify the relationship to other work, and list some open questions.

We firstly summarize the main results of the paper. In Theorem 10 and Corollary 11 we have determined explicitly and counted the quaternary Golay sequences and pairs of length 2^m $(m \geq 4)$ obtained by applying Lemmas 5 and 7 to the 512 non-standard quaternary ordered Golay seed pairs $(\boldsymbol{a}, \boldsymbol{b})$ of length 8 described in Theorem 2. These lemmas are equivalent to the iterative use of Budišin's construction, with arbitrary negative reversals of intermediate sequences allowed.

In Figure 2 we have identified a framework of constructions from which all known Golay sequences and pairs of length 2^m over $\mathbb{Z}_{2^h}$ can be obtained explicitly, and have shown the key importance of Turyn's construction and its variations. In Example 6 and its generalizations we have demonstrated that this framework is sufficiently powerful to produce further quaternary Golay sequences and pairs of length 2^m $(m \geq 7)$ that cannot be obtained by any other known construction.

We next describe the relationship to other work. Schmidt [15, Theorem 7] recently gave an algebraic normal form construction for "near-complementary sequences", based in part on earlier work of Parker and Tellambura [13], and remarked [15, p. 3230] that it could be applied to the Golay sequences of Theorem 2 "to obtain an explicit construction for Golay sequences of length 2^m, where $m > 3$". However neither [15] nor [13] gives details of the resulting sequences, and moreover carrying out the indicated procedure would lead only to the forms (13) and (14) of Theorem 10 (corresponding to the application of Lemma 5) and not to the forms (15) and (16) (corresponding to Lemma 7, in which arbitrary negative reversals of intermediate sequences are allowed).

Borwein and Ferguson [1] considered the Golay sequences and pairs that can be obtained from an arbitrary initial Golay pair $(\boldsymbol{a}, \boldsymbol{b})$ by the iterative use of Budišin's construction, including the effect of (negative) reversal of intermediate sequences. Indeed, we have adopted their matrix notation to describe constructed sequences. However [1] deals exclusively with binary sequences, and the only known binary length 2^m Golay pairs are standard pairs. In that case (negative) reversal of intermediate sequences does not produce any additional Golay sequences or pairs, as noted at the start of Section IV-E. Theorem 4.6 of [1] counts the number of binary ordered Golay pairs of length $2^m n$ that can be derived from an initial binary Golay pair of length n, but does not give an explicit algebraic normal form for the case $n = 2^r$ and once again deals only with the binary case, which is considerably less complex than the quaternary case considered here. (Strictly, the count of [1, Theorem 4.6] is an upper bound since it is not proved there that the counted sequences or pairs are distinct.)

After submission of the original manuscript we were able to obtain more detailed results on the generalizations of Example 6 discussed in Section IV-D. These are reported in [6].

We conclude with some open questions:

1) Are the minimum counts of non-standard length 32 and 64 quaternary Golay sequences and pairs in Table I exact (see the discussion at the end of Section V)?
2) What underlies the shared autocorrelation property of the quaternary Golay sequences (4)? Are there further examples of Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$ having the shared autocorrelation property (apart from trivial liftings and linear transformations of (4))? If so, this would allow the construction of further infinite families of non-standard Golay sequences and pairs via a new cross-over of autocorrelation functions (see the procedure of Section V).
3) Are there any non-standard binary length 2^m Golay pairs, arising either from a shared autocorrelation property of standard binary Golay sequences or in some other

way?

4) The algebraic normal forms for non-standard Golay sequences derived in Theorem 10 are rather complex, in contrast to those for standard Golay sequences in (1). Is there a better way to describe non-standard Golay pairs than by using the algebraic normal form?

REFERENCES

[1] P.B. Borwein and R.A. Ferguson, "A complete description of Golay pairs of length up to 100," *Math. Comp.*, vol. 73, pp. 967–985, 2004.

[2] S.Z. Budišin, "New complementary pairs of sequences," *Electron. Lett.*, vol. 26, pp. 881–883, 1990.

[3] R. Craigen, W. Holzmann, and H. Kharaghani, "Complex Golay sequences: structure and applications," *Discrete Math.*, vol. 252, pp. 73–89, 2002.

[4] J.A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2397–2417, 1999.

[5] F. Fiedler and J. Jedwab, "How do more Golay sequences arise?," *IEEE Trans. Inform. Theory*, vol. 52, pp. 4261–4266, 2006.

[6] F. Fiedler, J. Jedwab, and M.G. Parker, "A multi-dimensional approach to the construction and enumeration of Golay complementary sequences," *J. Combin. Theory (A)*, submitted.

[7] M.J.E. Golay, "Multislit spectroscopy," *J. Opt. Soc. Amer.*, vol. 39, pp. 437–444, 1949.

[8] M.J.E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 82–87, 1961.

[9] M.J.E. Golay, "Note on 'Complementary series'," *Proc. IRE*, vol. 50, pp. 84, 1962.

[10] W.H. Holzmann and H. Kharaghani, "A computer search for complex Golay sequences," *Australasian J. Combin.*, vol. 10, pp. 251–258, 1994.

[11] Y. Li and W.B. Chu, "More Golay sequences," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1141–1145, 2005.

[12] Y. Li and Y.-C. Kao, "Structures of non-GDJ Golay sequences," in *IEEE Int. Symp. Inform. Theory 2005, Adelaide*, pp. 378–381, 2005.

[13] M.G. Parker and C. Tellambura, "Generalised Rudin-Shapiro constructions," in *International Workshop on Coding and Cryptography 2001, Paris, eds. D. Augot and C. Carlet*, 2001.

[14] K.G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 104–120, 2000.

[15] K.-U. Schmidt, "On cosets of the generalized first-order Reed-Muller code with low PMEPR," *IEEE Trans. Inform. Theory*, vol. 52, pp. 3220–3232, 2006.

[16] R.J. Turyn, "Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings," *J. Combin. Theory (A)*, vol. 16, pp. 313–333, 1974.

[17] G.R. Welti, "Quaternary codes for pulsed radar," *IRE Trans. Inf. Theory*, vol. IT-6, pp. 400–408, 1960.

Frank Fiedler is a good guy.

Jonathan Jedwab received the B.A. degree in mathematics and the Diploma in mathematical statistics from Cambridge University, Cambridge, U.K., in 1986 and 1987, respectively, and the Ph.D. degree in mathematics from the University of London, London, U.K., in 1991. He was at Hewlett-Packard Laboratories, U.K., for 14 years in a mathematics consultancy group, where he worked particularly with digital communications engineers. In 2003, he moved to Vancouver, BC, Canada, to take up a position in the Department of Mathematics, Simon Fraser University, Burnaby, BC. His current research interests include applying discrete mathematics to solve theoretical and practical problems in digital communication, especially by using the results of exploratory computation. He is a named inventor on 23 granted and 5 pending patents.

Matthew Parker is really rather strange.